Nessus 4.4
Installationshandbuch

14. Juni 2011

(Revision 9)

Copyright © 2011 Tenable Network Security, Inc. Alle Rechte vorbehalten. Tenable Network Security und Nessus sind eingetragene Marken von Tenable Network Security, Inc. ProfessionalFeed ist eine Marke von Tenable Network Security, Inc. Alle anderen Produkte und Dienstleistungen sind Marken ihrer jeweiligen Eigentümer.

Tenable Network Security, Inc. • 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046, USA • +1 410 872 0555 • sales@tenable.com • www.tenable.com

Inhaltsverzeichnis

Einleitung **5**
Unterstützte Betriebssysteme 5
Regeln und Konventionen 5

Hintergrund **6**

Voraussetzungen **8**
Nessus UNIX 8
Nessus Windows 8

Bereitstellungsoptionen **8**

Bezug von Sicherheitslücken-Plugins **8**
Welcher Feed ist für Sie geeignet? 9
HomeFeed *9*
ProfessionalFeed *9*

IPv6-Unterstützung **10**

UNIX/Linux **10**
Upgrade ausführen 10
Installation 18
Konfiguration 23
Die wichtigsten Nessus-Verzeichnisse *23*
Einen Nessus-Benutzer erstellen *23*
Plugin-Aktivierungscode installieren *25*
Den Nessus-Daemon starten 27
Den Nessus-Daemon beenden 28
Befehlszeilenoptionen für nessusd 29
Verbindung mit einem Client herstellen 30
Plugins aktualisieren 31
Wie oft soll ich meine Plugins aktualisieren? *31*
Plugins automatisch aktualisieren *31*
Plugin-Updates mit cron planen *32*
Plugins über Webproxys aktualisieren *32*
Nessus entfernen 33

Windows **36**
Upgrade ausführen 36
Upgrade von Nessus 4.0 - 4.0.x ausführen *36*
Upgrade von Nessus 3.0 - 3.0.x ausführen *36*
Upgrade von Nessus 3.2 und höher ausführen *37*
Installation 37
Nessus herunterladen *37*
Installation *37*
Fragen zur Installation *38*
Die wichtigsten Nessus-Verzeichnisse *41*

Copyright © 2002-2011 Tenable Network Security, Inc.

Konfiguration....41
Nessus Server Manager....41
Den Nessus-Standardport ändern....43
Nessus-Installation registrieren....43
Aktivierungscodes zurücksetzen....45
Nessus-Benutzer erstellen und verwalten....45
Remoteverbindungen zulassen....45
Benutzerkonten hinzufügen....45
Hostbasierte Firewalls....48
Den Nessus-Daemon starten....49
Plugin-Updates ausführen....50
Wie oft soll ich meine Plugins aktualisieren?....51
Plugins über Webproxys aktualisieren....51
Nessus entfernen....51

Mac OS X....52
Upgrade ausführen....52
Installation....52
Konfiguration....55
Nessus Server Manager....55
Nessus-Installation registrieren....57
Aktivierungscodes zurücksetzen....58
Nessus-Benutzer erstellen und verwalten....58
Remoteverbindungen zulassen....58
Benutzerkonten hinzufügen....59
Den Nessus-Daemon starten....60
Plugin-Updates ausführen....60
Wie oft soll ich meine Plugins aktualisieren?....61
Nessus entfernen....61

Nessus-Daemon konfigurieren (für fortgeschrittene Benutzer)....61

Nessus mit einem angepassten SSL-Zertifikat konfigurieren....67

Nessus ohne Internetzugang....68
Nessus-Scanner registrieren....68
Aktuelle Plugins beziehen und installieren....71
Windows....71
Linux, Solaris und FreeBSD....71
Mac OS X....72

Mit SecurityCenter arbeiten....72
SecurityCenter im Überblick....72
Nessus für die Kooperation mit SecurityCenter konfigurieren....73
UNIX/Mac OS X....73
Windows....73
Nessus für das Horchen als Netzwerk-Daemon konfigurieren....73
Benutzerkonten unter Windows hinzufügen....73
Den Nessus-Dienst unter Windows aktivieren....74
Hostbasierte Firewalls....75
SecurityCenter für die Kooperation mit Nessus konfigurieren....75

Copyright © 2002-2011 Tenable Network Security, Inc.

Problembehandlung bei Nessus für Windows 76
Installations- und Upgradeprobleme 76
Probleme beim Scannen 76

Weitere Informationen 78

Lizenzerklärungen Dritter 79

Wissenswertes zu Tenable Network Security 83

Copyright © 2002-2011 Tenable Network Security, Inc.

EINLEITUNG

Das vorliegende Dokument beschreibt die Installation und Konfiguration des Sicherheitslückenscanners **Nessus 4.4** von Tenable Network Security. Wir freuen uns über Ihre Anmerkungen und Vorschläge zu diesem Produkt. Schicken Sie einfach eine E-Mail an support@tenable.com.

Tenable Network Security, Inc. hat den Sicherheitslückenscanner Nessus entwickelt und vertreibt ihn. Tenable arbeitet nicht nur fortlaufend an der Optimierung der Nessus-Engine, sondern entwickelt auch die meisten für diesen Scanner erhältlichen Plugins sowie Compliancetests und eine Vielzahl von Auditrichtlinien.

Im vorliegenden Dokument werden Voraussetzungen und Bereitstellungsoptionen beschrieben. Außerdem finden Sie hier eine Anleitung der Installationsschritte. Grundlegende Kenntnisse zu UNIX und zu Sicherheitslückenscannern werden dabei vorausgesetzt.

Seit Nessus 4.4 erfolgt die Benutzerverwaltung des Nessus-Servers über eine Weboberfläche. Ein NessusClient wird nicht mehr benötigt. Der Scanner kann zwar weiterhin über den NessusClient bedient werden, es wird aber für den Client keine Updates mehr geben.

UNTERSTÜTZTE BETRIEBSSYSTEME

Nessus wird für eine Vielzahl von Betriebssystemen und Plattformen angeboten und unterstützt:

- Debian 5 (i386 und x86-64)
- Fedora Core 12, 13 und 14 (i386 und x86-64)
- FreeBSD 8 (i386 und x86-64)
- Mac OS X 10.4, 10.5 und 10.6 (i386, x86-64, ppc)
- Red Hat ES 4 / CentOS 4 (i386)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 und x86-64)
- Red Hat ES 6 / CentOS 6 (i386 und x86-64) [Server, Desktop, Workstation]
- Solaris 10 (sparc)
- SuSE 9.3 (i386)
- SuSE 10.0 und 11 (i386 und x86-64)
- Ubuntu 8.04, 9.10, 10.04 und 10.10 (i386 und x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2, Vista und 7 (i386 und x86-64)

REGELN UND KONVENTIONEN

Das vorliegende Dokument wurde aus einer ursprünglich auf Englisch verfassten Version übersetzt. Teilweise wurden Texte auf Englisch beibehalten, wenn diese in englischer Form im Produkt erscheinen.

In der gesamten Dokumentation werden Dateinamen, Daemons und ausführbare Dateien in einer Schriftart wie **`courier bold`** angezeigt (Beispiel: **`setup.exe`**).

Befehlszeilenoptionen und Suchbegriffe werden ebenfalls in der Schriftart **`courier bold`** angezeigt. Die Befehlszeilen sind teils mit, teils ohne Befehlszeilen-Prompt und den Ausgabetext des betreffenden Befehls aufgeführt. Häufig ist der Befehl **fett** gedruckt, um zu verdeutlichen, was der Benutzer eingegeben hat. Es folgt ein Beispiel für die Ausführung des UNIX-Befehls **`pwd`**:

Copyright © 2002-2011 Tenable Network Security, Inc.

```
# pwd
/opt/nessus/
#
```

Wichtige Hinweise und Aspekte werden durch dieses Symbol und graue Textfelder hervorgehoben.

Tipps, Beispiele und Best Practices (Empfehlungen) werden durch dieses Symbol und weißen Text auf blauem Grund hervorgehoben.

HINTERGRUND

Nessus ist ein leistungsfähiger, aktueller und benutzerfreundlicher Netzwerksicherheits-scanner. Er zählt gegenwärtig in der gesamten Security-Branche zu den besten Produkten seiner Art und wird durch professionelle Datensicherheitsorganisationen wie das SANS Institute beworben und gefördert. Nessus ermöglicht es Ihnen, einen Remote-Audit Ihres Netzwerks durchzuführen und festzustellen, ob Unbefugte in das Netzwerk eingedrungen sind oder ein Missbrauch der Netzwerkfunktionen aufgetreten ist. Nessus bietet zudem die Möglichkeit, ein bestimmtes System lokal auf Sicherheitslücken, die Erfüllung von Compliance-Anforderungen, eine Verletzung von Inhaltsrichtlinien usw. zu prüfen.

- **Intelligentes Scannen.** Anders als bei vielen anderen Sicherheitsscannern wird von Nessus nichts als gegeben vorausgesetzt. Es wird z. B. nicht erwartet, dass ein bestimmter Dienst über einen bestimmten Port ausgeführt wird. Wenn Sie also Ihren Webserver über den Port 1234 betreiben, wird dies von Nessus erkannt, und die Sicherheitstests werden entsprechend ausgeführt. Soweit dies möglich ist, wird versucht, eine Sicherheitslücke durch tatsächliche Nutzung zu bestätigen. In Fällen, in denen eine solche Vorgehensweise nicht zuverlässig ist oder negative Auswirkungen auf das Ziel haben kann, nutzt Nessus unter Umständen ein Serverbanner, um das Vorhandensein einer Sicherheitslücke zu ermitteln. In diesem Fall geht aus dem Ausgabebericht eindeutig hervor, ob diese Methode verwendet wurde.

- **Modulare Architektur.** Die Client/Server-Architektur bietet die erforderliche Flexibilität, um den Scanner (Server) bereitzustellen und eine Verbindung mit dem GUI (grafische Benutzeroberfläche, Client) herzustellen, der auf einem beliebigen Computer in einem Webbrowser ausgeführt wird. Diese Vorgehensweise senkt die Verwaltungskosten, da mehrere Clients auf denselben Server zugreifen können.

- **CVE-Kompatibilität.** Die meisten Plugins verweisen auf die CVE, damit Administratoren weitere Informationen zu veröffentlichten Sicherheitslücken abrufen können. Häufig sind auch Referenzen in BugTraq (BID), OSVDB und bei anderen Anbietern von Sicherheitswarnungen angegeben.

- **Plugin-Architektur.** Alle Sicherheitstests werden als externes Plugin entwickelt und dann einer von 42 Plugin-Familien zugeordnet. Auf diese Weise können Sie ganz einfach eigene Tests hinzufügen, bestimmte Plugins auswählen oder eine ganze Familie nutzen, ohne den Code der Nessus-Server-Engine (**`nessusd`**) lesen zu müssen. Eine vollständige Liste der Nessus-Plugins finden Sie unter http://www.nessus.org/plugins/index.php?view=all.

Copyright © 2002-2011 Tenable Network Security, Inc.

- **NASL.** Der Nessus-Scanner umfasst die NASL-Sprache (Nessus Attack Scripting Language). NASL wurde speziell zur schnellen und einfachen Entwicklung von Sicherheitstests entworfen.

- **Aktuelle Sicherheitslücken-Datenbank.** Tenable legt bei der Entwicklung von Sicherheitstests den Schwerpunkt auf neu entdeckte Sicherheitslücken. Die Datenbank mit den Sicherheitstests wird täglich aktualisiert. Die aktuellsten Sicherheitstests stehen unter http://www.nessus.org/scripts.php zum Download bereit.

- **Gleichzeitiger Test mehrerer Hosts.** Abhängig von der Konfiguration Ihres Nessus-Scannersystems können Sie eine große Zahl Hosts gleichzeitig testen.

- **Intelligente Diensterkennung.** Nessus setzt nicht voraus, dass sich die Zielhosts nach den von der IANA zugewiesenen Portnummern richten. Ein FTP-Server, der über einen anderen als den Standardport ausgeführt wird (z. B. Port 31337), wird ebenso erkannt wie ein Webserver, der Port 8080 statt Port 80 nutzt.

- **Mehrere Dienste.** Wenn zwei oder mehr Webserver auf einem Host ausgeführt werden (z. B. einer auf Port 80 und ein zweiter auf Port 8080), dann werden sie alle von Nessus erkannt und getestet.

- **Plugin-Kooperation.** Die von Nessus-Plugins ausgeführten Tests kooperieren, d. h. es werden keine unnötigen Tests ausgeführt. Wenn Ihr FTP-Server keine anonymen Anmeldungen bietet, dann werden für anonyme Anmeldungen relevante Sicherheitstests nicht ausgeführt.

- **Umfassende Berichterstattung.** Mit Nessus erfahren Sie nicht nur, welche Sicherheitslücken in Ihrem Netzwerk vorhanden sind und welches Risikoausmaß sie jeweils darstellen (niedrig, moderat, hoch oder kritisch), sondern erhalten auch Informationen zu Lösungen, um diese Lücken zu schließen.

- **Vollständige SSL-Unterstützung.** Nessus kann auch Dienste testen, die über SSL vermittelt werden (z. B. HTTPS, SMTPS, IMAPS usw.).

- **Smart-Plugins (optional).** Nessus stellt selbstständig fest, mit welchen Plugins ein Remotehost getestet werden soll – und mit welchen nicht. Beispielsweise werden sendmail-Sicherheitslücken von Nessus nicht für Postfix ausgeführt. Diese Option wird als Optimierung bezeichnet.

- **Nichtdestruktiver Betrieb (optional).** Einige Tests wirken sich negativ auf bestimmte Netzwerkdienste aus. Wenn Sie das Risiko eines Dienstausfalls in Ihrem Netzwerk nicht eingehen möchten, aktivieren Sie die Nessus-Option „Safe Checks" („Sichere Tests"). In diesem Fall nutzt Nessus Banner zur Überprüfung darauf, ob eine Sicherheitslücke vorhanden ist, statt Fehler tatsächlich zu nutzen.

- **Offenes Forum.** Sie haben einen Bug gefunden? Oder eine Frage zu Nessus? Beteiligen Sie sich am Forum unter https://discussions.nessus.org/.

Copyright © 2002-2011 Tenable Network Security, Inc.

VORAUSSETZUNGEN

Tenable empfiehlt für den Betrieb von Nessus mindestens 2 GB Arbeitsspeicher. Für umfangreichere Scans mehrerer Netzwerke werden mindestens 3 GB empfohlen, wobei für einen flüssigen Betrieb bis zu 4 GB erforderlich sein können.

Als Prozessor wird ein Pentium 3 mit 2 GHz oder höher empfohlen. Für die Ausführung im Mac OS X wird ein Intel® Dualcore-Prozessor mit 2 GHz oder höher empfohlen.

Nessus kann in einer VMware-Instanz ausgeführt werden. Wenn die virtuelle Maschine jedoch die Netzadressübersetzung (Network Address Translation, NAT) für die Verbindung mit dem Netzwerk verwendet, kann dies zahlreiche Sicherheitstests, die Hostauflistung und die Betriebssystemerkennung von Nessus beeinträchtigen.

NESSUS UNIX

Für die Installation von Nessus unter UNIX/Linux müssen verschiedene Bibliotheken vorhanden sein. Viele Betriebssysteme installieren diese standardmäßig, weswegen eine separate Installation in der Regel nicht erforderlich ist:

- OpenSSL (z. B. openssl, libssl, libcrypto)
- zlib
- GNU C-Bibliothek (d. h. libc)

NESSUS WINDOWS

Microsoft hat an Windows XP SP2 und höher (und zwar sowohl bei der Home- als auch bei der Professional-Version) Änderungen vorgenommen, die die Leistungsfähigkeit von Nessus Windows beeinträchtigen können. Um die Leistungsfähigkeit und die Zuverlässigkeit von Scans zu steigern, wird dringend empfohlen, Nessus Windows auf einem Serverprodukt der Microsoft Windows-Familie (z. B. Windows Server 2003) zu installieren. Weitere Informationen zu diesem Thema finden Sie unter „Nessus: Problembehandlung unter Windows".

BEREITSTELLUNGSOPTIONEN

Für die Bereitstellung von Nessus sind Kenntnisse in den Bereichen Routing, Filter und Firewallrichtlinien häufig sehr nützlich. Wir empfehlen, Nessus so bereitzustellen, dass eine ausreichende IP-Konnektivität zu den zu scannenden Netzwerken besteht. Die Bereitstellung hinter einem NAT-Gerät wird nur für Scans im internen Netzwerk empfohlen. Wenn ein Sicherheitslückenscan einen NAT- oder Anwendungsproxy passieren muss, kann der Test verfälscht werden. In solchen Fällen kann es zu Fehlalarmen, aber auch zum Übersehen von Sicherheitslücken kommen. Außerdem können Personal Firewalls oder Desktop-Firewalls auf dem System, auf dem Nessus ausgeführt wird, die Wirksamkeit eines remote ausgeführten Sicherheitslückenscans erheblich beeinträchtigen.

Hostbasierte Firewalls können Sicherheitslückenscans im Netzwerk stören. Je nach Konfiguration Ihrer Firewall können die Probes (Testdaten) eines Nessus-Scans verhindert, beschädigt oder verborgen werden.

BEZUG VON SICHERHEITSLÜCKEN-PLUGINS

Tag für Tag werden zahlreiche neue Sicherheitslücken von Anbietern, Forschern und anderen Quellen publik gemacht. Ziel von Tenable ist es, Tests für neu veröffentlichte

Copyright © 2002-2011 Tenable Network Security, Inc.

Sicherheitslücken möglichst schnell zu testen und verfügbar zu machen. Im Normalfall geschieht dies innerhalb von 24 Stunden nach der Bekanntgabe. Ein Testmodul für eine bestimmte Sicherheitslücke heißt in der Terminologie des Nessus-Scanners „Plugin". Eine vollständige Liste der Nessus-Plugins finden Sie unter http://www.nessus.org/plugins/index.php?view=all. Tenable verteilt Nessus-Plugins für die aktuellsten Sicherheitslücken auf zweierlei Weise: als ProfessionalFeed und als HomeFeed.

Plugins werden direkt von Tenable heruntergeladen. Dies geschieht über einen automatisierten Prozess in Nessus. Nach dem Download überprüft Nessus die digitalen Signaturen aller heruntergeladenen Plugins, um die Dateiintegrität sicherzustellen. Für Nessus-Installationen ohne Internetzugang gibt es einen Offlineupdateprozess, mit dem sich sicherstellen lässt, dass der Scanner auf dem aktuellen Stand bleibt.

Bei Nessus 4 müssen Sie sich für einen Plugin-Feed registrieren und die Plugins aktualisieren, bevor Sie Nessus starten und die Scanoberfläche von Nessus angezeigt wird. Das Plugin-Update läuft nach der Erstregistrierung des Scanners im Hintergrund und kann mehrere Minuten dauern.

Welcher Feed ist für Sie geeignet?

Eine konkrete Anleitung zur Konfiguration von Nessus für den Bezug des HomeFeed bzw. des ProfessionalFeed finden Sie weiter unten in diesem Dokument. Lesen Sie die folgenden Abschnitte, um festzustellen, welcher Nessus-Feed für Ihre Umgebung geeignet ist:

HomeFeed

Der HomeFeed ist für Benutzer gedacht, die Nessus zu Hause und nicht kommerziell einsetzen. Neue Plugins für die aktuellsten Sicherheitslücken werden sofort für HomeFeed-Benutzer freigegeben. Die Nutzung des HomeFeed ist kostenfrei. Allerdings gibt es für den HomeFeed eine separate Lizenz, die der Benutzer akzeptieren muss. Besuchen Sie zur Registrierung des HomeFeed die Seite http://www.nessus.org/register/. Dort registrieren Sie Ihre Nessus-Kopie zur Verwendung des HomeFeed. Den Aktivierungscode, den Sie während der Registrierung erhalten, verwenden Sie, wenn Sie Nessus für den Bezug von Updates konfigurieren. HomeFeed-Benutzer erhalten keinen Zugang zum Tenable Support Portal, zu Compliancetests und zu den Richtlinien für Inhaltsaudits.

ProfessionalFeed

Wenn Sie Nessus zu kommerziellen Zwecken (z. B. für das Consulting) oder in Geschäfts- oder Behördenumgebungen einsetzen, müssen Sie einen ProfessionalFeed erwerben. Neue Plugins für die aktuellsten Sicherheitslücken werden sofort für ProfessionalFeed-Benutzer freigegeben. SecurityCenter-Kunden beziehen den ProfessionalFeed automatisch und müssen einen zusätzlichen Feed nur dann erwerben, wenn sie einen Nessus-Scanner einsetzen, der nicht durch SecurityCenter verwaltet wird.

Tenable bietet über das Tenable Support Portal oder via E-Mail kommerziellen Support für ProfessionalFeed-Kunden, die Nessus 4 einsetzen. Ebenfalls im ProfessionalFeed enthalten ist eine Anzahl hostbasierter Compliancetests für UNIX und Windows. Diese sind sehr nützlich bei der Ausführung von Compliance-Audits nach den Vorgaben von SOX, FISMA oder FDCC.

Sie können einen ProfessionalFeed entweder über den Onlinestore von Tenable unter https://store.tenable.com/ oder bei einem der autorisierten ProfessionalFeed-Partner erwerben. Danach erhalten Sie von Tenable einen Aktivierungscode. Diesen Code verwenden Sie bei der Updatekonfiguration Ihrer Nessus-Kopie.

Copyright © 2002-2011 Tenable Network Security, Inc.

Wenn Sie Nessus in Verbindung mit Tenable SecurityCenter verwenden, erhält SecurityCenter Zugriff auf den ProfessionalFeed und aktualisiert Ihre Nessus-Scanner automatisch.

Bestimmte Netzwerkgeräte, die eine zustandsbezogene Inspektion ausführen (z. B. Firewalls, Lastausgleichsmodule oder Intrusion-Detection- bzw. Intrusion-Prevention-Systeme), können negativ reagieren, wenn sie bei einem Scan überprüft werden. Nessus bietet eine Reihe von Optimierungsoptionen, mit denen sich die Auswirkungen des Scannens solcher Geräte einschränken lassen. Allerdings lassen sich Probleme in Verbindung mit dem Scannen solcher Netzwerkgeräte am besten vermeiden, indem Sie einen authentifizierten Scan durchführen.

IPV6-UNTERSTÜTZUNG

Seit Version 3.2 BETA unterstützt Nessus das Scannen IPv6-basierter Ressourcen. Viele Betriebssysteme und Geräte bieten mittlerweile standardmäßig aktivierte IPv6-Unterstützung. Um Scans von IPv6-Ressourcen durchzuführen, muss mindestens eine IPv6-Schnittstelle auf dem Host, auf dem Nessus installiert ist, konfiguriert sein. Zudem muss sich Nessus in einem IPv6-fähigen Netzwerk befinden (Nessus kann IPv6-Ressourcen über IPv4 nicht scannen, aber IPv6-Schnittstellen mithilfe authentifizierter Scans über IPv4 auflisten). Bei Scans werden sowohl die vollständige als auch die verkürzte IPv6-Notation unterstützt.

Unter Microsoft Windows fehlen einige wichtige APIs, die für den Nachbau von IPv6-Paketen erforderlich sind (z. B. zum Abruf der MAC-Adresse des Routers, der Routingtabelle usw.). Hierdurch wird ein ordnungsgemäßes Funktionieren des Portscanners verhindert. Tenable arbeitet gegenwärtig an Verbesserungen, mit denen diese API-Beschränkungen in zukünftigen Nessus-Versionen umgangen werden können.

UNIX/LINUX

UPGRADE AUSFÜHREN

In diesem Abschnitt wird erläutert, wie ein Upgrade einer vorhandenen Nessus-Installation ausgeführt wird.

In der folgenden Tabelle finden Sie Hinweise zu Upgrades für den Nessus-Server auf allen bisher unterstützten Plattformen. Zuvor erstellte Konfigurationseinstellungen und Benutzer werden unverändert übernommen.

Stellen Sie sicher, dass eine laufende Ausführung von Scans abgeschlossen wurde, bevor Sie **`nessusd`** anhalten.

Spezielle Upgradehinweise finden Sie jeweils in einer auf das Beispiel folgenden Anmerkung.

Copyright © 2002-2011 Tenable Network Security, Inc.

Plattform	Upgradeanleitung
Red Hat ES 4 (32-Bit), ES 5 (32- und 64-Bit)	
Upgradebefehle	# **service nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Red Hat-Version: # **rpm -Uvh Nessus-4.4.0-es4.i386.rpm** # **rpm -Uvh Nessus-4.4.0-es5.i386.rpm** # **rpm -Uvh Nessus-4.4.0-es5.x86_64.rpm** Starten Sie nach Abschluss des Upgrades den Dienst **nessusd** über folgenden Befehl neu: # **service nessusd start**
Beispielausgabe	# **service nessusd stop** Shutting down Nessus services: [OK] # **rpm -Uvh Nessus-4.4.0-es4.i386.rpm** Preparing... ### [100%] Shutting down Nessus services: 1:Nessus ### [100%] nessusd (Nessus) 4.4.0 for Linux (C) 1998 – 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /sbin/service nessusd start # **service nessusd start** Starting Nessus services: [OK] #
Fedora Core 12, 13 und 14 (32- und 64-Bit)	
Upgradebefehle	# **service nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Fedora Core-Version: # **rpm -Uvh Nessus-4.4.0-fc12.i386.rpm**

Copyright © 2002-2011 Tenable Network Security, Inc.

	# **rpm -Uvh Nessus-4.4.0-fc12.x86_64.rpm** # **rpm -Uvh Nessus-4.4.0-fc14.i386.rpm** # **rpm -Uvh Nessus-4.4.0-fc14.x86_64.rpm** Starten Sie nach Abschluss des Upgrades den Dienst **nessusd** über folgenden Befehl neu: # **service nessusd start**
Beispielausgabe	# **service nessusd stop** Shutting down Nessus services: [OK] # **rpm -Uvh Nessus-4.4.0-fc12.i386.rpm** Preparing... ### [100%] Shutting down Nessus services: 1:Nessus ### [100%] nessusd (Nessus) 4.4.0 for Linux (C) 1998 – 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /sbin/service nessusd start # **service nessusd start** **Starting Nessus services: [OK]** #
SuSE 9.3 (32-Bit), 10 (32- und 64-Bit)	
Upgradebefehle	# **service nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete SuSE-Version: # **rpm -Uvh Nessus-4.4.0-suse9.3.i586.rpm** # **rpm -Uvh Nessus-4.4.0-suse10.0.i586.rpm** # **rpm -Uvh Nessus-4.4.0-suse10.x86_64.rpm** Starten Sie nach Abschluss des Upgrades den Dienst **nessusd** über folgenden Befehl neu: # **service nessusd start**
Beispielausgabe	# **service nessusd stop** Shutting down Nessus services: [OK] # **rpm -Uvh Nessus-4.4.0-suse10.0.i586.rpm**

Copyright © 2002-2011 Tenable Network Security, Inc.

	Preparing... ## [100%] Shutting down Nessus services: 1:Nessus ## [100%] nessusd (Nessus) 4.4.0 for Linux (C) 1998 - 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /sbin/service nessusd start # **service nessusd start** Starting Nessus services: [OK] #
Debian 5 (32- und 64-Bit)	
Upgradebefehle	# **/etc/init.d/nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Debian-Version: # **dpkg -i Nessus-4.4.0-debian5_i386.deb** # **dpkg -i Nessus-4.4.0-debian5_amd64.deb** # **/etc/init.d/nessusd start**
Beispielausgabe	# **/etc/init.d/nessusd stop** # **dpkg -i Nessus-4.4.0-debian5_i386.deb** (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 4.4.0 (using Nessus-4.4.0-debian5_i386.deb) ... Shutting down Nessus : . Unpacking replacement nessus ... Setting up nessus (4.4.0) ... nessusd (Nessus) 4.4.0. for Linux (C) 2009 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded

Copyright © 2002-2011 Tenable Network Security, Inc.

	- Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start # **/etc/init.d/nessusd start** Starting Nessus : . #
Ubuntu 8.04, 9.10, 10.04 und 10.10 (32- und 64-Bit)	
Upgradebefehle	# **/etc/init.d/nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Ubuntu-Version: # **dpkg -i Nessus-4.4.0-ubuntu804_i386.deb** # **dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb** # **dpkg -i Nessus-4.4.0-ubuntu910_i386.deb** # **dpkg -i Nessus-4.4.0-ubuntu910_amd64.deb** # **dpkg -i Nessus-4.4.0-ubuntu1010_amd64.deb** # **dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb** # **/etc/init.d/nessusd start**
Beispielausgabe	# **/etc/init.d/nessusd stop** # **dpkg -i Nessus-4.4.0-ubuntu804_i386.deb** (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 4.4.0 (using Nessus-4.4.0-ubuntu810_i386.deb) ... Shutting down Nessus : . Unpacking replacement nessus ... Setting up nessus (4.4.0) ... nessusd (Nessus) 4.4.0. for Linux (C) 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start

Copyright © 2002-2011 Tenable Network Security, Inc.

	# **/etc/init.d/nessusd start** Starting Nessus : . #
Solaris 10 (sparc)	
Upgradebefehle	# **/etc/init.d/nessusd stop** # **pkginfo | grep nessus** Nachfolgend gezeigt ist eine Beispielausgabe für den vorherigen Befehl, der das Nessus-Paket anzeigt: application TNBLnessus The Nessus Network Vulnerability Scanner Führen Sie zum Entfernen des Nessus-Pakets von einem Solaris-System folgenden Befehl aus: # **pkgrm <package name>** # **gunzip Nessus-4.x.x-solaris-sparc.pkg.gz** # **pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg** The following packages are available: 1 TNBLnessus-4-2-0 TNBLnessus (sparc) 4.4.0 Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]: 1 # **/etc/init.d/nessusd start**
Beispielausgabe	# **/etc/init.d/nessusd stop** # **pkginfo | grep nessus** application TNBLnessus The Nessus Network Vulnerability Scanner # **pkgrm TNBLnessus** (output redacted) ## Updating system information. Removal of <TNBLnessus> was successful. # **gunzip Nessus-4.4.0-solaris-sparc.pkg.gz** # **pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg** The following packages are available: 1 TNBLnessus The Nessus Network Vulnerability Scanner (sparc) 4.4.0 Select package(s) you wish to process (or 'all' to

Copyright © 2002-2011 Tenable Network Security, Inc.

	process all packages). (default: all) [?,??,q]: 1 Processing package instance <TNBLnessus> from </export/home/cbf/TENABLE/Nessus-4.4.0-solaris- sparc.pkg> The Nessus Network Vulnerability Scanner (sparc) 4.4.0 ## Processing package information. ## Processing system information. 13 package pathnames are already properly installed. ## Verifying disk space requirements. ## Checking for conflicts with packages already installed. ## Checking for setuid/setgid programs. This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <TNBLnessus> [y,n,?]y Installing The Nessus Network Vulnerability Scanner as <TNBLnessus> ## Installing part 1 of 1. (output redacted) ## Executing postinstall script. - Please run /opt/nessus/sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start Installation of <TNBLnessus> was successful. # **/etc/init.d/nessusd start** #
Hinweise	Zur Aktualisierung von Nessus unter Solaris müssen Sie die vorhandene Version zunächst deinstallieren und dann das neueste Release installieren. Bei diesem Vorgang werden die Konfigurationsdateien sowie Dateien, die nicht Bestandteil der Ursprungsinstallation waren, nicht entfernt. Wenn Bibliothekskompatibilitätsfehler auftreten, stellen Sie sicher, dass Sie den aktuellen Solaris Recommended Patch Cluster von Sun aufgespielt haben.

Copyright © 2002-2011 Tenable Network Security, Inc.

FreeBSD 8 (32- und 64-Bit)	
Upgradebefehle	# **killall nessusd** # **pkg_info** Durch diesen Befehl wird eine Liste aller installierten Pakete und ihrer Beschreibungen erstellt. Nachfolgend gezeigt ist eine Beispielausgabe für den vorherigen Befehl, der das Nessus-Paket anzeigt: Nessus-4.2.2 A powerful security scanner Entfernen Sie das Nessus-Paket mithilfe des folgenden Befehls: # **pkg_delete <package name>** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete FreeBSD-Version: # **pkg_add Nessus-4.4.0-fbsd8.tbz** # **pkg_add Nessus-4.4.0-fbsd8.amd64.tbz** # **/usr/local/nessus/sbin/nessusd -D**
Beispielausgabe	# **killall nessusd** # **pkg_delete Nessus-4.2.2** # **pkg_add Nessus-4.4.0-fbsd8.tbz** nessusd (Nessus) 4.4.0. for FreeBSD (C) 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /usr/local/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /usr/local/etc/rc.d/nessusd.sh start # **/usr/local/nessus/sbin/nessusd -D** nessusd (Nessus) 4.4.0. for FreeBSD (C) 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded #

Copyright © 2002-2011 Tenable Network Security, Inc.

Hinweise	Zur Aktualisierung von Nessus unter FreeBSD müssen Sie die vorhandene Version zunächst deinstallieren und dann das neueste Release installieren. Bei diesem Vorgang werden die Konfigurationsdateien sowie Dateien, die nicht Bestandteil der Ursprungsinstallation waren, nicht entfernt.

INSTALLATION

Die erstmalige Aktualisierung und Verarbeitung der Plugins durch Nessus kann mehrere Minuten in Anspruch nehmen. Der Webserver zeigt die Meldung „Nessus is initializing" („Nessus wird initialisiert") an und wird nach Abschluss des Vorgangs neu geladen.

Laden Sie die aktuelle Nessus-Version von http://www.nessus.org/download/ oder über das Tenable Support Portal herunter. Überprüfen Sie die Integrität des Installationspakets, indem Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei **`MD5.asc`** (hier) angegebenen Prüfsumme vergleichen.

Sofern nicht anders angegeben, müssen alle Befehle als „root" Benutzer des Systems ausgeführt werden. Normale Benutzerkonten verfügen gewöhnlich nicht über die zur Installation dieser Software erforderlichen Berechtigungen.

In der folgenden Tabelle finden Sie Hinweise zur Installation des Nessus-Servers auf allen unterstützten Plattformen. Spezielle Installationshinweise finden Sie jeweils in einer auf das Beispiel folgenden Anmerkung.

Plattform	Installationsanleitung
Red Hat ES 4 (32-Bit), ES 5 (32- und 64-Bit)	

Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Red Hat-Version:
	
	`# rpm -ivh Nessus-4.4.0-es4.i386.rpm`
	`# rpm -ivh Nessus-4.4.0-es5.i386.rpm`
	`# rpm -ivh Nessus-4.4.0-es5.x86_64.rpm`

Beispielausgabe	`# rpm -ivh Nessus-4.4.0-es4.i386.rpm`
	`Preparing...`
	`########################################### [100%]`
	`1:Nessus`
	`########################################### [100%]`
	`nessusd (Nessus) 4.4.0. for Linux`
	`(C) 1998 - 2011 Tenable Network Security, Inc.`
	
	`- Please run /opt/nessus//sbin/nessus-adduser to add a user`
	`- Register your Nessus scanner at http://www.nessus.org/register/ to obtain`

Copyright © 2002-2011 Tenable Network Security, Inc.

	all the newest plugins - You can start nessusd by typing /sbin/service nessusd start #
Fedora Core 12, 13 und 14 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Fedora Core-Version: # **rpm -ivh Nessus-4.4.0-fc12.i386.rpm** # **rpm -ivh Nessus-4.4.0-fc12.x86_64.rpm** # **rpm -ivh Nessus-4.4.0-fc14.i386.rpm** # **rpm -ivh Nessus-4.4.0-fc14.x86_64.rpm**
Beispielausgabe	# **rpm -ivh Nessus-4.4.0-fc12.i386.rpm** Preparing... ## [100%] 1:Nessus ## [100%] nessusd (Nessus) 4.4.0. for Linux (C) 1998 - 2011 Tenable Network Security, Inc. - Please run /opt/nessus//sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /sbin/service nessusd start #
SuSE 9.3 (32-Bit), 10 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete SuSE-Version: # **rpm -ivh Nessus-4.4.0-suse9.3.i586.rpm** # **rpm -ivh Nessus-4.4.0-suse10.0.i586.rpm** # **rpm –ivh Nessus-4.4.0-suse10.x86_64.rpm**
Beispielausgabe	# **rpm -ivh Nessus-4.4.0-suse10.0.i586.rpm** Preparing... ## [100%] 1:Nessus ## [100%] Nessusd {Nessus} 4.4.0. for Linux (C) 1998 - 2011 Tenable Network Security, Inc. - Please run /opt/nessus//sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain

Copyright © 2002-2011 Tenable Network Security, Inc.

	all the newest plugins - You can start nessusd by typing /etc/rc.d/nessusd start #
Debian 5 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Debian-Version: # **dpkg -i Nessus-4.4.0 -debian5_i386.deb** # **dpkg -i Nessus-4.4.0 -debian5_amd64.deb**
Beispielausgabe	# **dpkg -i Nessus-4.4.0-debian5_i386.deb** Selecting previously deselected package nessus. (Reading database ... 36954 files and directories currently installed.) Unpacking nessus (from Nessus-4.4.0-debian5_i386.deb) ... Setting up nessus (4.4.0) ... nessusd (Nessus) 4.4.0. for Linux (C) 1998 - 2011 Tenable Network Security, Inc. - Please run /opt/nessus/sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start #
Hinweise	Der Nessus-Daemon kann erst gestartet werden, nachdem Nessus registriert und die Plugins heruntergeladen wurden. Standardmäßig wird Nessus mit einem leeren Plugin-Satz ausgeliefert. Wenn Sie versuchen, Nessus ohne Plugins zu starten, wird die folgende Ausgabe zurückgegeben: # **/etc/init.d/nessusd start** Starting Nessus : . # Missing plugins. Attempting a plugin update... Your installation is missing plugins. Please register and try again. To register, please visit http://www.nessus.org/register/
Ubuntu 8.04, 9.10, 10.04 und 10.10 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Ubuntu-Version: # **dpkg -i Nessus-4.4.0-ubuntu804_i386.deb** # **dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb** # **dpkg -i Nessus-4.4.0-ubuntu910_i386.deb**

Copyright © 2002-2011 Tenable Network Security, Inc.

	# dpkg -i Nessus-4.4.0-ubuntu910_amd64.deb **# dpkg -i Nessus-4.4.0-ubuntu1010_amd64.deb** **# dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb**
Beispielausgabe	**# dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb** Selecting previously deselected package nessus. (Reading database ... 32444 files and directories currently installed.) Unpacking nessus (from Nessus-4.4.0-ubuntu804_amd64.deb) ... Setting up nessus (4.4.0) ... - Please run /opt/nessus/sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start #
Solaris 10 (sparc)	
Installationsbefehl	**# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz** **# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg** The following packages are available: 1 TNBLnessus The Nessus Network Vulnerability Scanner (sparc) 4.4.0 Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:1
Beispielausgabe	**# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz** **# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg** The following packages are available: 1 TNBLnessus The Nessus Network Vulnerability Scanner (sparc) 4.4.0 Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:1 Processing package instance <TNBLnessus> from </tmp/Nessus-4.4.0-solaris-sparc.pkg> The Nessus Network Vulnerability Scanner(sparc) 4.4.0 ## Processing package information. ## Processing system information. ## Verifying disk space requirements. ## Checking for conflicts with packages already installed. ## Checking for setuid/setgid programs.

Copyright © 2002-2011 Tenable Network Security, Inc.

	This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <TNBLnessus> [y,n,?]y Installing The Nessus Network Vulnerability Scanner as <TNBLnessus> ## Installing part 1 of 1. (output redacted) ## Executing postinstall script. - Please run /opt/nessus/sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start Installation of <TNBLnessus> was successful. # **/etc/init.d/nessusd start** #
Hinweise	Wenn Bibliothekskompatibilitätsfehler auftreten, stellen Sie sicher, dass Sie den aktuellen Solaris Recommended Patch Cluster von Sun aufgespielt haben.
FreeBSD 8 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete FreeBSD-Version: # **pkg_add Nessus-4.4.0-fbsd8.tbz** # **pkg_add Nessus-4.4.0-fbsd8.amd64.tbz**
Beispielausgabe	# **pkg_add Nessus-4.4.0-fbsd8.tbz** nessusd (Nessus) 4.4.0 for FreeBSD (C) 1998 - 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /usr/local/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain

Copyright © 2002-2011 Tenable Network Security, Inc.

	all the newest plugins - You can start nessusd by typing /usr/local/etc/rc.d/nessusd.sh start #

Nach der Installation von Nessus wird eine Anpassung der mitgelieferten Konfigurationsdatei an Ihre Umgebung empfohlen. Die Vorgehensweise wird im Abschnitt „Konfiguration" beschrieben.

Nessus muss in **`/opt/nessus`** installiert sein. Allerdings wird auch eine Konfiguration unterstützt, in der **`/opt/nessus`** eine symbolische Verknüpfung (Symlink) ist, die auf eine andere Speicherposition verweist.

KONFIGURATION

Die wichtigsten Nessus-Verzeichnisse

In der folgenden Tabelle sind die Installationsposition und wichtige Verzeichnisse aufgelistet, die von Nessus verwendet werden:

Nessus-Stammverzeichnis	Nessus-Unterverzeichnisse	Zweck
UNIX-Distributionen		
Red Hat, SuSE, Debian, Ubuntu, Solaris: `/opt/nessus`	**`./etc/nessus/`**	Konfigurationsdateien
	`./var/nessus/users/<username>/kbs/`	Auf Festplatte gespeicherte User-Knowledge-Base
FreeBSD: `/usr/local/nessus`	**`./lib/nessus/plugins/`**	Nessus-Plugins
Mac OS X: `/Library/Nessus/run`	**`./var/nessus/logs/`**	Nessus-Logdateien

Einen Nessus-Benutzer erstellen

Mindestens ein Nessus-Benutzer muss erstellt werden, damit Clientprogramme sich bei Nessus anmelden können, um Scans zu starten und Ergebnisse abzurufen.

Sofern nicht anders angegeben, müssen alle Befehle als „root" Benutzer des Systems ausgeführt werden.

Verwenden Sie zur Kennwortauthentifizierung den Befehl **`nessus-adduser`**, um Benutzer hinzuzufügen. Der erste hinzugefügte Benutzer sollte möglichst der Administrator sein.

Für jeden Nessus-Benutzer gibt es eine Anzahl Regeln, mit denen gesteuert wird, was der Benutzer scannen darf und was nicht. Diese Regeln werden als „Benutzerregeln" bezeichnet. Standardmäßig kann ein neuer Benutzer, für den bei der Erstellung in Nessus keine Regeln eingegeben wurden, beliebige IP-Adressbereiche scannen. Nessus unterstützt einen globalen

Copyright © 2002-2011 Tenable Network Security, Inc.

Regelsatz, der in der Datei „**nessusd.rules**" abgelegt ist. Die dort vermerkten Regeln haben Vorrang vor allen benutzerspezifischen Regeln. Wenn Sie Regeln für einen bestimmten Benutzer erstellen, tun Sie nichts anderes, als die vorhandenen globalen Regeln zu verfeinern.

```
# /opt/nessus/sbin/nessus-adduser
Login : sumi_nessus
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins,
      etc...) (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that sumi_nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)



Login             : sumi_nessus
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
User added
#
```

Ein Benutzer, der kein Administrator ist, kann weder Plugins in Nessus hochladen noch einen Remoteneustart durchführen (was nach einem Plugin-Upload erforderlich ist) oder die Einstellung **max_hosts/max_checks** in **nessusd.conf** außer Kraft setzen. **Wenn für den Benutzer eine Verwendung von SecurityCenter vorgesehen ist, muss es sich um einen Administrator handeln.** SecurityCenter verwaltet eine eigene Benutzerliste und legt Berechtigungen für seine Benutzer fest.

Ein einzelner Nessus-Scanner kann einen komplexen Aufbau mit mehreren Benutzern unterstützen. Denkbar ist beispielsweise, dass in einem Unternehmen mehrere Mitarbeiter Zugriff auf denselben Nessus-Scanner haben, mit diesem aber jeweils unterschiedliche IP-Bereiche gescannt werden sollen. Für solche Fälle lassen sich die zu scannenden IP-Bereiche einschränken.

Das folgende Beispiel veranschaulicht die Erstellung eines zweiten Nessus-Benutzers mit Kennwortauthentifizierung und Benutzerregeln, mit denen der Benutzer lediglich das Klasse-B-Netzwerk 172.20.0.0/16 scannen kann. Weitere Beispiele und die Syntax für Benutzerregeln entnehmen Sie den Manpages für **nessus-adduser**.

```
# /opt/nessus/sbin/nessus-adduser
Login : tater_nessus
Login password :
```

Copyright © 2002-2011 Tenable Network Security, Inc.

```
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins,
       etc...) (y/n) [n]: n
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that tater_nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
accept 172.20.0.0/16
deny 0.0.0.0/0



Login             : tater_nessus
Password          : ***********
Rules             :
accept 172.20.0.0/16
deny 0.0.0.0/0
Is that ok ? (y/n) [y] y
User added
#
```

Zur Anzeige der Manpage für nessus-adduser(8) müssen Sie unter bestimmten Betriebssystemen die folgenden Befehle ausführen:

```
# export MANPATH=/opt/nessus/man
# man nessus-adduser
```

In Nessus 4.0.x und früher war die Authentifizierung zwischen dem NessusClient und dem Nessus-Server mithilfe von SSL-Zertifikaten konfigurierbar. Dies ist nun nicht mehr erforderlich, weil der Zugriff auf den Nessus-Server via SSL-Webauthentifizierung und nicht mehr über einen separaten NessusClient erfolgt. Die einzige Ausnahme hierfür ist die Authentifizierung zwischen SecurityCenter und dem Nessus-Server, da SecurityCenter als Nessus-Client agiert. Informationen zur Authentifizierung mit SSL-Zertifikaten für diese Konfiguration finden Sie in der Dokumentation zu SecurityCenter.

Plugin-Aktivierungscode installieren

Wenn Sie Tenable SecurityCenter verwenden, werden der Aktivierungscode und Plugin-Updates über SecurityCenter verwaltet. Zur Kommunikation mit SecurityCenter muss Nessus gestartet werden, was gewöhnlich ohne einen gültigen Aktivierungscode und Plugins nicht möglich ist. Damit diese Anforderung von Nessus ignoriert wird und ein Start erfolgen kann (und die Plugin-Updates aus SecurityCenter abgerufen werden können), führen Sie folgenden Befehl aus:

Copyright © 2002-2011 Tenable Network Security, Inc.

```
# nessus-fetch --security-center
```

Geben Sie dann unmittelbar nach Ausführung des obigen Befehls „**nessus-fetch**" den zum Starten des Nessus-Servers erforderlichen Befehl ein. Der Nessus-Server kann SecurityCenter nun über die SecurityCenter-Weboberfläche hinzugefügt werden. Informationen zur Konfiguration eines zentralen Plugin-Feeds für mehrere Nessus-Scanner finden Sie in der SecurityCenter-Dokumentation.

Vor dem ersten Start von Nessus müssen Sie einen Aktivierungscode eingeben, um die aktuellen Plugins herunterladen zu können. Das erstmalige Herunterladen und Verarbeiten von Plugins kann zusätzliche Zeit in Anspruch nehmen, bevor der Nessus-Server einsatzbereit ist.

Je nach Abonnement haben Sie einen Aktivierungscode erhalten, der Sie zum Bezug von ProfessionalFeed- oder HomeFeed-Plugins berechtigt. Bei diesem Vorgang wird Ihr Nessus-Scanner auf alle verfügbaren Plugins synchronisiert. Aktivierungscodes sind 16 oder 20 Zeichen lange Zeichenfolgen, die alphanummerische Zeichen und Bindestriche enthalten.

Geben Sie zur Installation des Aktivierungscodes folgenden Befehl auf dem System ein, auf dem Nessus ausgeführt wird (hierbei ist **<license code>** der Ihnen übermittelte Registrierungscode):

Linux und Solaris:

```
# /opt/nessus/bin/nessus-fetch --register <Activation Code>
```

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --register <Activation Code>
```

Nach der erstmaligen Registrierung lädt Nessus die Plugins von plugins.nessus.org, plugins-customers.nessus.org oder plugins-us.nessus.org im Hintergrund herunter und kompiliert sie. Wenn dieser Vorgang zum ersten Mal ausgeführt wird, kann es bis zu zehn Minuten dauern, bis der Nessus-Server betriebsbereit ist. Sobald die Meldung „nessusd is ready" („nessusd ist bereit") im Log **nessusd.messages** erscheint, akzeptiert der Nessus-Server Clientverbindungen, und die Scanoberfläche wird verfügbar. Beim Aktivierungscode braucht die Groß-/Kleinschreibung **nicht** beachtet werden.

Eine Internetverbindung ist für diesen Schritt erforderlich. Wenn Sie Nessus auf einem System ohne Internetverbindung ausführen, gehen Sie zur Installation Ihres Aktivierungscodes so vor wie im Abschnitt „Nessus ohne Internetzugang" beschrieben.

Das nachfolgende Beispiel zeigt die Schritte zum Registrieren des Plugin-Aktivierungscodes, zum Abrufen der aktuellen Plugins von der Nessus-Website und zum Überprüfen eines erfolgreichen Downloads.

Copyright © 2002-2011 Tenable Network Security, Inc.

```
# /opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
# cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "200912160934";
PLUGIN_FEED = "ProfessionalFeed (Direct)";
```

Mithilfe der Datei **plugin_feed_info.inc**, die sich im Verzeichnis **/opt/nessus/lib/nessus/plugins/** befindet, wird überprüft, über welchen Plugin-Satz und welchen Feed Sie verfügen. Sehen Sie sich diese Datei an, um sicherzustellen, dass Sie mit den aktuellsten Plugins arbeiten.

DEN NESSUS-DAEMON STARTEN

Nessus startet erst nach der Registrierung des Scanners und dem Plugin-Download. SecurityCenter-Benutzer, die den folgenden Befehl eingeben, müssen weder einen Registrierungscode angeben noch Plugins herunterladen:

```
# nessus-fetch --security-center
```

Starten Sie den Nessus-Dienst als „root" mit dem folgenden Befehl:

Linux und Solaris:

```
# /opt/nessus/sbin/nessus-service -D
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service -D
```

Nachfolgend gezeigt ist eine Beispielausgabe für den Start von **nessusd** unter Red Hat:

```
# /opt/nessus/sbin/nessus-service -D

nessusd (Nessus) 4.4.0 for Linux
(C) 1998 - 2011 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
#
```

Wenn Sie die Ausgabe des Befehls unterdrücken möchten, verwenden Sie die Option „**-q**" wie folgt:

Copyright © 2002-2011 Tenable Network Security, Inc.

Linux und Solaris:

```
# /opt/nessus/sbin/nessus-service -q -D
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service -q -D
```

Alternativ kann Nessus abhängig von der Betriebssystemplattform mit dem folgenden Befehl gestartet werden:

Betriebssystem	Startbefehl `nessusd`
Red Hat	`# /sbin/service nessusd start`
Fedora Core	`# /sbin/service nessusd start`
SuSE	`# /etc/rc.d/nessusd start`
Debian	`# /etc/init.d/nessusd start`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh start`
Solaris	`# /etc/init.d/nessusd start`
Ubuntu	`# /etc/init.d/nessusd start`

Nach dem Start des Dienstes **nessusd** ist die Erstinstallation und -konfiguration des Nessus 4-Scanners für SecurityCenter-Benutzer abgeschlossen. Wenn Sie SecurityCenter nicht zur Verbindung mit **nessusd** verwenden, führen Sie die nachfolgend beschriebenen Schritte aus, um den Plugin-Aktivierungscode zu installieren.

Den Nessus-Daemon beenden

Wenn Sie den Dienst **nessusd** aus irgendeinem Grund beenden müssen, verwenden Sie den folgenden Befehl, um Nessus anzuhalten und alle laufenden Scans direkt zu beenden:

```
# killall nessusd
```

Wir empfehlen jedoch, stattdessen die folgenden, weniger drastisch agierenden Skripts zum Beenden zu verwenden:

Betriebssystem	Stoppbefehl `nessusd`
Red Hat	`# /sbin/service nessusd stop`

Copyright © 2002-2011 Tenable Network Security, Inc.

Fedora Core	`# /sbin/service nessusd stop`
SuSE	`# /etc/rc.d/nessusd stop`
Debian	`# /etc/init.d/nessusd stop`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh stop`
Solaris	`# /etc/init.d/nessusd stop`
Ubuntu	`# /etc/init.d/nessusd stop`

BEFEHLSZEILENOPTIONEN FÜR NESSUSD

Zusätzlich zur einfachen Ausführung des **nessusd**-Servers gibt es eine Reihe von Befehlszeilenoptionen, die je nach Bedarf verwendet werden können. Die folgende Tabelle enthält Informationen zu diesen optionalen Befehlen.

Optionen	Beschreibung
-c <config-file>	Beim Start des **nessusd**-Servers kann mithilfe dieser Option die zu verwendende serverseitige **nessusd**-Konfigurationsdatei angegeben werden. Dies ermöglicht die Verwendung einer alternativen Konfigurationsdatei anstelle der Standarddatei **/opt/nessus/etc/nessus/nessusd.conf** (bzw. **/usr/local/nessus/etc/nessus/nessusd.conf** für FreeBSD).
-a <address>	Beim Start des **nessusd**-Servers kann mithilfe dieser Option festgelegt werden, dass der Server nur auf Verbindungen mit der Adresse **<address>** horcht. Hierbei handelt es sich um eine IP-Adresse (d. h. nicht um einen Computernamen). Diese Option ist nützlich, wenn Sie **nessusd** auf einem Gateway ausführen und vermeiden möchten, dass von außen eine Verbindung mit Ihrem **nessusd** hergestellt werden kann.
-S <ip[,ip2,...]>	Beim Start des **nessusd**-Servers erzwingen Sie mit diesem Befehl die Festlegung der IP-Absenderadresse von Verbindungen, die von Nessus während des Scanvorgangs hergestellt werden, auf **<ip>**. Diese Option ist nur dann von Nutzen, wenn Sie einen Multihomed-Computer mit mehreren öffentlichen IP-Adressen einsetzen, die statt der Standardadresse verwendet werden sollen. Damit eine solche Konfiguration funktioniert, muss der Host, auf dem **nessusd** ausgeführt wird, über mehrere Netzwerkkarten mit entsprechend festgelegten IP-Adressen verfügen.
-p <port-number>	Beim Start des **nessusd**-Servers kann dieser mithilfe dieser Option angewiesen werden, auf Clientverbindungen über den Port **<port-number>** statt über den Standardport 1241 zu horchen.

Copyright © 2002-2011 Tenable Network Security, Inc.

-D	Beim Start des **nessusd**-Servers wird mithilfe dieser Option festgelegt, dass der Server im Hintergrund ausgeführt wird (Daemon-Modus).
-v	Zeigt die Versionsnummer an und wird dann beendet.
-l	Zeigt die Plugin-Feedlizenz an und wird dann beendet.
-h	Zeigt eine Befehlszusammenfassung an und wird dann beendet.
--ipv4-only	Es wird nur auf dem IPv4-Socket gehorcht.
--ipv6-only	Es wird nur auf dem IPv6-Socket gehorcht.
-q	Betrieb im „stillen" Modus (alle Meldungen an **stdout** werden unterdrückt).
-R	Erzwingt eine Neuverarbeitung der Plugins.
-t	Überprüft die Zeitstempel aller Plugins beim Start.
-K	Hiermit wird ein Masterkennwort für den Scanner festgelegt.

Wenn ein Masterkennwort festgelegt wird, verschlüsselt Nessus alle Richtlinien und die darin enthaltenen Anmeldedaten mit dem durch den Benutzer angegebenen Schlüssel (dieser ist erheblich sicherer als der Standardschlüssel). Wird ein Kennwort festgelegt, dann werden Sie beim Start über die Weboberfläche aufgefordert, es einzugeben.

ACHTUNG: Wenn das Masterkennwort festgelegt wurde und dann verloren geht, kann es weder durch Ihren Administrator noch durch den Tenable-Support wiederhergestellt werden.

Nachfolgend gezeigt ist ein Einsatzbeispiel:

Linux:

```
# /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
```

VERBINDUNG MIT EINEM CLIENT HERSTELLEN

Wenn die Installation abgeschlossen wurde und die Plugins aktualisiert und verarbeitet wurden, ist der Nessus-Server zur Herstellung einer Verbindung mit einem Client bereit.

Copyright © 2002-2011 Tenable Network Security, Inc.

Tenable unterstützt den Zugriff auf den Nessus-Server über einen nativen Webserver (Standardport: 8834), die Befehlszeile oder die SecurityCenter-Oberfläche (diese wird im Abschnitt „Mit SecurityCenter arbeiten" ausführlich beschrieben). Informationen zum Zugriff auf die Benutzeroberfläche des Webservers und die Nutzung der Befehlszeile finden Sie im „Nessus Benutzerhandbuch", das unter http://www.tenable.com/products/nessus/documentation verfügbar ist.

Die erstmalige Aktualisierung und Verarbeitung der Plugins durch Nessus kann mehrere Minuten in Anspruch nehmen. Der Webserver ist nachfolgend verfügbar. Eine Anmeldung ist allerdings erst nach Abschluss der Plugin-Verarbeitung möglich.

PLUGINS AKTUALISIEREN

Mit dem folgenden Befehl aktualisieren Sie den Nessus-Scanner auf die aktuellsten Plugins:

Linux und Solaris:

```
# /opt/nessus/sbin/nessus-update-plugins
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-update-plugins
```

Da täglich neue Sicherheitslücken erkannt und veröffentlicht werden, werden jeden Tag neue Nessus-Plugins entwickelt. Damit Ihr Nessus-Scanner auf dem aktuellen Stand bleibt und stets die neuesten Plugins benutzt, müssen Sie Ihre Plugins häufig aktualisieren, denn nur so kann der Scanner zuverlässig arbeiten.

Wie oft soll ich meine Plugins aktualisieren?

Im Allgemeinen ist eine tägliche Aktualisierung der Nessus-Plugins für die meisten Organisationen ausreichend. Wenn Sie jedoch stets die aktuellsten Plugins benötigen und eine fortlaufende Aktualisierung während des gesamten Tages wünschen, können Sie in einem 4-Stunden-Turnus Aktualisierungen durchführen. Eine häufigere Aktualisierung bringt praktisch keinen zusätzlichen Nutzen.

Plugins automatisch aktualisieren

Seit Version 3.0 ruft Nessus die aktuellsten Plugins regelmäßig automatisch ab. Hierzu wird die Option **auto_update** in der Datei **nessusd.conf** verwendet. Standardmäßig hat diese Option den Wert „yes" („ja"). Mithilfe der Option **auto_update_delay** wird festgelegt, wie häufig die Plugins aktualisiert werden. Die Angabe erfolgt dabei in Stunden. Der Standardwert liegt bei 24 Stunden, der Mindestwert bei vier Stunden. Der Updatevorgang für die Plugins erfolgt nach Verstreichen der festgelegten Anzahl Stunden nach dem Start von **nessusd** und anschließend im gleichen Intervall.

Damit diese Option einwandfrei funktioniert, müssen Sie sicherstellen, dass der Aktivierungscode für den Plugin-Feed im Scanner korrekt festgelegt ist. Dies können Sie mit dem folgenden Befehl überprüfen:

Linux und Solaris:

```
# /opt/nessus/bin/nessus-fetch --check
```

Copyright © 2002-2011 Tenable Network Security, Inc.

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --check
```

Automatische Plugin-Updates werden nur gestartet, wenn

- die Option **auto_update** in der Datei **nessusd.conf** den Wert „yes" hat,
- der Aktivierungscode für den Plugin-Feed über **nessus-fetch** in diesem Scanner registriert wurde, während eine Internetverbindung aktiv war und
- der Scanner nicht über Tenable SecurityCenter fernverwaltet wird.

Beachten Sie, dass nach erfolgter Offline-Registrierung des Plugin-Feeds Nessus nicht in der Lage ist, die aktuellsten Plugins automatisch zu beziehen.

Plugin-Updates mit cron planen

Wenn Ihre Organisation aus technischen oder logistischen Gründen keine automatische Aktualisierung der Nessus-Plugins zulassen kann, können Sie zu diesem Zweck auch einen Cronjob einrichten.

Führen Sie die folgenden Schritte durch, um eine nächtliche Aktualisierung Ihrer Plugins via cron auszuführen:

- Geben Sie **su root** (bzw. **sudo bash**, falls Sie über sudo-Berechtigungen verfügen) ein, um „root" zu werden.
- Geben Sie als „root" **crontab -e** ein, um die Crontab des „root" Benutzers zu bearbeiten.
- Fügen Sie Ihrer Crontab folgende Zeile hinzu:
  ```
  28 3 * * * /opt/nessus/sbin/nessus-update-plugins
  ```

Bei obiger Konfiguration wird der Befehl **nessus-update-plugins** jede Nacht um 3:28 Uhr aufgerufen. Da **nessusd** von **nessus-update-plugins** automatisch neu gestartet wird, ohne laufende Scans zu unterbrechen, müssen Sie nichts weiter tun.

Wenn Sie cron für Plugin-Updates konfigurieren, achten Sie darauf, **das Update nicht zur vollen Stunde zu starten.** Wählen Sie bei der Einrichtung des Zeitplans einen beliebigen Zeitpunkt aus, der im Zeitraum zwischen fünf Minuten nach und 55 Minuten vor der vollen Stunde liegt, und planen Sie Ihren Download für diesen Zeitpunkt.

Seit Version 4.4 kann Nessus Plugins auch bei laufendem Scan aktualisieren. Nach Abschluss des Updates verwenden alle nachfolgenden Scans den aktualisierten Plugin-Satz. Ein Benutzer muss sich während dieses Vorgangs nicht von der Weboberfläche abmelden.

Plugins über Webproxys aktualisieren

Unter UNIX-basierten Betriebssystemen unterstützt Nessus die Produktregistrierung und Plugin-Updates über Webproxys, die eine Standardauthentifizierung erfordern. Die Proxyeinstellungen finden Sie in der Datei **/opt/nessus/etc/nessus/nessus-fetch.rc**. Vier Zeilen sind für die Steuerung proxybasierter Verbindungen relevant. Sie sind nachfolgend mit einer Beispielsyntax aufgeführt:

Copyright © 2002-2011 Tenable Network Security, Inc.

```
proxy=myproxy.example.com
proxy_port=8080
proxy_username=juser
proxy_password=squirrel
```

Für die Anweisung „**proxy**" können ein DNS-Hostname oder eine IP-Adresse verwendet werden. In der Datei **nessus-fetch.rc** darf nur ein Proxy angegeben sein. Zusätzlich kann erforderlichenfalls eine **user_agent** Anweisung angegeben werden, die die Verwendung eines benutzerdefinierten HTTP-Benutzeragenten in Nessus erzwingt.

NESSUS ENTFERNEN

In der folgenden Tabelle finden Sie Hinweise zum Entfernen des Nessus-Servers auf allen unterstützten Plattformen. Mit Ausnahme von Mac OS X werden bei diesem Vorgang weder Konfigurationsdateien noch Dateien entfernt, die nicht Bestandteil der Ursprungsinstallation waren. Dateien, die Bestandteil des Originalpakets waren, aber seit der Installation geändert wurden, werden ebenfalls nicht entfernt. Zur Entfernung der übrigen Dateien verwenden Sie den folgenden Befehl:

Linux und Solaris:

```
# rm -rf /opt/nessus
```

FreeBSD:

```
# rm -rf /usr/local/nessus/bin
```

Plattform	Deinstallationsanleitung
Red Hat ES 4 (32-Bit), ES 5 (32- und 64-Bit)	

Deinstallationsbefehl	Ermitteln Sie den Paketnamen:
	
	`# rpm -qa | grep Nessus`
	
	Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen:
	
	`# rpm -e <Package Name>`

Beispielausgabe	`# rpm -qa | grep -i nessus`
	`Nessus-4.4.0-es5`
	`# rpm -e Nessus-4.4.0-es5`
	`#`

Fedora Core 12, 13 und 14 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: `# rpm -qa | grep Nessus` Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen:

Copyright © 2002-2011 Tenable Network Security, Inc.

	# **rpm -e <Package Name>**
SuSE 9.3 (32-Bit), 10 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: # **rpm -qa | grep Nessus** Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen: # **rpm -e <Package Name>**
Debian 5 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: # **dpkg -l | grep -i nessus** Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen: # **dpkg -r <package name>**
Beispielausgabe	# **dpkg -l | grep nessus** ii nessus 4.4.0 Version 4 of the Nessus Scanner # **dpkg -r nessus** #
Ubuntu 8.04, 9.10, 10.04 und 10.10 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: # **dpkg -l | grep -i nessus** Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen: # **dpkg -r <package name>**
Beispielausgabe	# dpkg -l | grep -i nessus ii nessus 4.4.0 Version 4 of the Nessus Scanner #
Solaris 10 (sparc)	
Deinstallationsbefehl	Beenden Sie den **nessusd**-Dienst: # **/etc/init.d/nessusd stop**

Copyright © 2002-2011 Tenable Network Security, Inc.

	Ermitteln Sie den Paketnamen:
	
	`# pkginfo | grep –i nessus`
	
	Entfernen Sie das Nessus-Paket:
	
	`# pkgrm <package name>`

Beispielausgabe	Nachfolgend gezeigt ist eine Beispielausgabe für den vorherigen Befehl, der das Nessus-Paket anzeigt:
	
	`# pkginfo | grep –i nessus`
	
	`application TNBLnessus The Nessus Network Vulnerability Scanner`
	`# pkgrm TNBLnessus`
	`#`

FreeBSD 8 (32- und 64-Bit)	

Deinstallationsbefehl	Beenden Sie Nessus:
	
	`# killall nessusd`
	
	Ermitteln Sie den Paketnamen:
	
	`# pkg_info | grep -i nessus`
	
	Entfernen Sie das Nessus-Paket:
	
	`# pkg_delete <package name>`

Beispielausgabe	`# killall nessusd`
	
	`# pkg_info | grep -i nessus`
	`Nessus-4.4.0 A powerful security scanner`
	`# pkg_delete Nessus-4.4.0`
	`#`

Mac OS X	

Deinstallationsbefehl	Rufen Sie ein Terminalfenster auf. Wählen Sie hierzu unter „Programme" den Eintrag „Dienstprogramme" aus und klicken Sie dann auf „Terminal" oder „X11". Geben Sie am Shell-Prompt den Befehl „sudo" ein, um eine Root-Shell auszuführen, und entfernen Sie die Nessus-Verzeichnisse wie folgt:
	
	`$ sudo /bin/sh`
	`Password:`
	`# ls -ld /Library/Nessus`
	`# rm -rf /Library/Nessus`
	`# ls -ld /Library/Nessus`
	`# ls -ld /Applications/Nessus`

Copyright © 2002-2011 Tenable Network Security, Inc.

	`# rm -rf /Applications/Nessus`
	`# ls -ld /Applications/Nessus`
	`# ls -ld /Library/Receipts/Nessus*`
	`# rm -rf /Library/Receipts/Nessus*`
	`# ls -ld /Library/Receipts/Nessus*`
	`# exit`

Beispielausgabe	`$ sudo /bin/sh`
	`Password:`
	`# ls -ld /Library/Nessus`
	`drwxr-xr-x  6 root  admin  204 Apr  6 15:12 /Library/Nessus`
	`# rm -rf /Library/Nessus`
	`# ls -ld /Library/Nessus`
	`ls: /Library/Nessus: No such file or directory`
	`# ls -ld /Applications/Nessus`
	`drwxr-xr-x  4 root  admin  136 Apr  6 15:12 /Applications/Nessus`
	`# rm -rf /Applications/Nessus`
	`# ls -ld /Applications/Nessus`
	`# ls -ld /Library/Receipts/Nessus*`
	`drwxrwxr-x  3 root  admin  102 Apr  6 15:11 /Library/Receipts/Nessus Client.pkg`
	`drwxrwxr-x  3 root  admin  102 Apr  6 15:11 /Library/Receipts/Nessus Server.pkg`
	`# rm -rf /Library/Receipts/Nessus*`
	`# ls -ld /Library/Receipts/Nessus*`
	`ls: /Library/Receipts/Nessus*: No such file or directory`
	`# exit`
	`$`

Hinweise	Führen Sie diesen Vorgang nur aus, wenn Sie mit UNIX-Shell-Befehlen vertraut sind. Die „`ls`"-Befehle sind enthalten, um sicherzustellen, dass der Pfadname korrekt eingegeben wurde.

WINDOWS

UPGRADE AUSFÜHREN

Upgrade von Nessus 4.0 - 4.0.x ausführen

Beim Nessus-Upgrade von einer Version 4.x auf eine neuere 4.x-Distribution werden Sie im Verlauf des Upgradevorgangs gefragt, ob Sie alles im Nessus-Verzeichnis löschen möchten. Wenn Sie sich für diese Option entscheiden (indem Sie „Yes" auswählen), wird ein Deinstallationsprozess imitiert. In diesem Fall werden zuvor erstellte Benutzer, vorhandene Scanrichtlinien und Scanergebnisse entfernt, und die Registrierung des Scanners wird aufgehoben.

Upgrade von Nessus 3.0 - 3.0.x ausführen

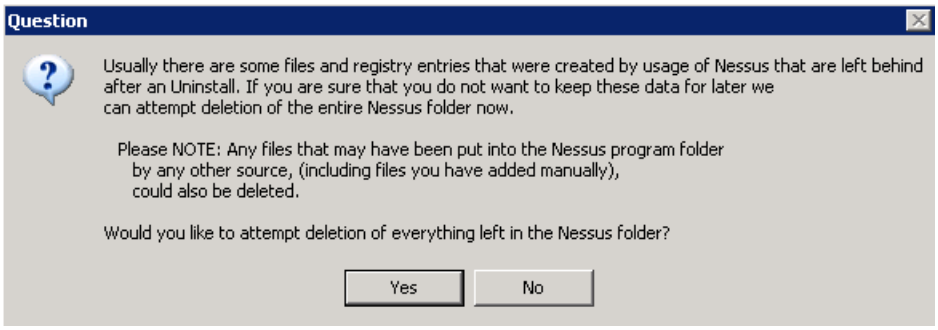
Ein direktes Upgrade von Nessus 3.0.x auf Nessus 4.x wird nicht unterstützt. Sie können allerdings als Zwischenschritt ein Upgrade auf Version 3.2 verwenden, um sicherzustellen, dass wichtige Scaneinstellungen und -richtlinien nicht verloren gehen. Wenn Sie die Scaneinstellungen nicht behalten möchten, deinstallieren Sie zunächst Nessus 3.x und installieren Sie Nessus 4 dann von Grund auf neu.

Copyright © 2002-2011 Tenable Network Security, Inc.

Wenn Sie sich für ein Upgrade auf Version 3.2 als Zwischenschritt entscheiden, finden Sie weitere Informationen im Nessus 3.2 Installationshandbuch.

Upgrade von Nessus 3.2 und höher ausführen

Wenn Sie Nessus 3.2 oder höher verwenden, können Sie das Nessus 4-Paket herunterladen und es installieren, ohne die vorhandene Version deinstallieren zu müssen. Alle früheren Berichte zu Sicherheitslückenscans und Scanrichtlinien werden auf Wunsch gespeichert und bleiben erhalten. Das folgende Dialogfeld wird während des Upgrades angezeigt, um dem Benutzer die Möglichkeit zu geben, die vorherige Installation zu speichern oder zu löschen:


Question
Usually there are some files and registry entries that were created by usage of Nessus that are left behind after an Uninstall. If you are sure that you do not want to keep these data for later we can attempt deletion of the entire Nessus folder now.
Please NOTE: Any files that may have been put into the Nessus program folder by any other source, (including files you have added manually), could also be deleted.
Would you like to attempt deletion of everything left in the Nessus folder?
Yes
No

Klicken Sie auf „Yes" („Ja"), wenn Nessus versuchen soll, den gesamten Nessus-Ordner sowie ggf. manuell hinzugefügte Dateien zu löschen, oder auf „No" („Nein"), wenn der Nessus-Ordner sowie die vorhandenen Scans, Berichte usw. beibehalten werden sollen. Nach der Installation der neuen Nessus-Version stehen diese Daten dann nach wie vor zur Anzeige und zum Export zur Verfügung.

Achtung: Wenn Sie „Yes" auswählen, werden alle Dateien im Nessus-Verzeichnis einschließlich der Logdateien, manuell hinzugefügter angepasster Plugins usw. gelöscht. Wählen Sie diese Option nur aus, wenn Sie sich ganz sicher sind!

INSTALLATION

Nessus herunterladen

Die aktuellste Version von Nessus steht unter http://www.nessus.org/download/ zum Download bereit. Nessus 4.4 ist für Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista und Windows 7 verfügbar. Überprüfen Sie die Integrität des Installationspakets, indem Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei `MD5.asc` (hier) angegebenen Prüfsumme vergleichen.

Die Größen und Namen von Nessus-Distributionsdateien unterschiedlicher Versionen variieren geringfügig. Im Allgemeinen liegt die Dateigröße jedoch immer bei etwa 12 MB.

Installation

Nessus wird als ausführbare Installationsdatei vertrieben. Speichern Sie die Datei auf dem System, auf dem die Installation ausgeführt werden soll, oder auf einem freigegebenen Laufwerk, auf das vom System aus zugegriffen werden kann.

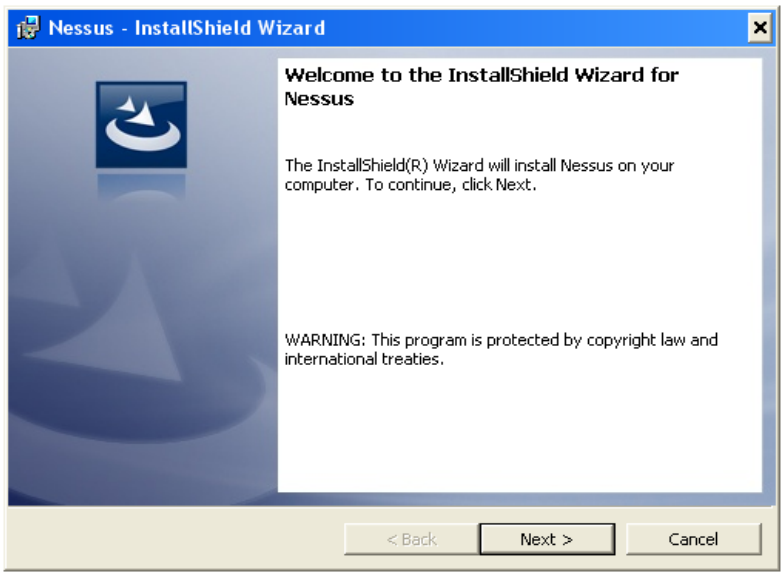
Sie müssen Nessus mit einem Konto mit Administratorrechten installieren; ein normales Benutzerkonto ist nicht ausreichend. Wenn Fehlermeldungen in Bezug auf Berechtigungen,

Copyright © 2002-2011 Tenable Network Security, Inc.

Zugriffsverweigerungen oder Fehler auftreten, die auf mangelnde Zugriffsberechtigung hindeuten, stellen Sie sicher, dass Sie ein Konto mit Administratorrechten verwenden. Erhalten Sie diese Fehlermeldungen bei der Verwendung der Befehlszeilendienstprogramme, dann führen Sie **`cmd.exe`** unter einem ausführenden Konto mit Administratorrechten aus.

Bestimmte Antivirensoftware kann Nessus möglicherweise als Wurm oder eine andere Form von Schadsoftware klassifizieren. Dies ist durch die große Anzahl der TCP-Verbindungen bedingt, die bei einem Scan erzeugt wird. Wenn Ihre Antivirensoftware eine Warnung ausgibt, klicken Sie auf „Zulassen", damit der Nessus-Scan fortgesetzt werden kann. In den meisten Antivirenpaketen können der Ausnahmeliste Prozesse hinzugefügt werden. Fügen Sie dieser Liste **`Nessus.exe`** und **`Nessus-service.exe`** hinzu, um solche Warnmeldungen in Zukunft zu vermeiden.

Fragen zur Installation

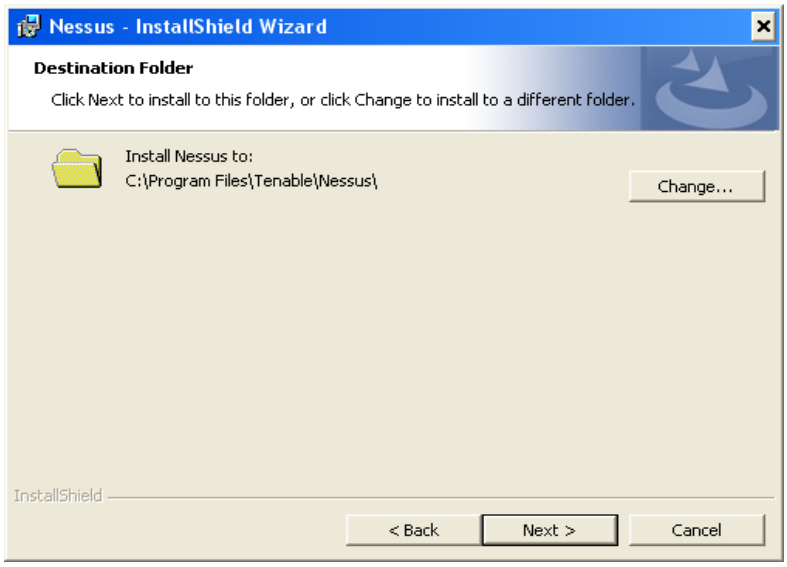

Nessus - InstallShield Wizard
Welcome to the InstallShield Wizard for Nessus
The InstallShield(R) Wizard will install Nessus on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

Während des Installationsvorgangs von Nessus werden einige Benutzerangaben angefordert. Zu Beginn müssen Sie dem Lizenzvertrag zustimmen:

Copyright © 2002-2011 Tenable Network Security, Inc.

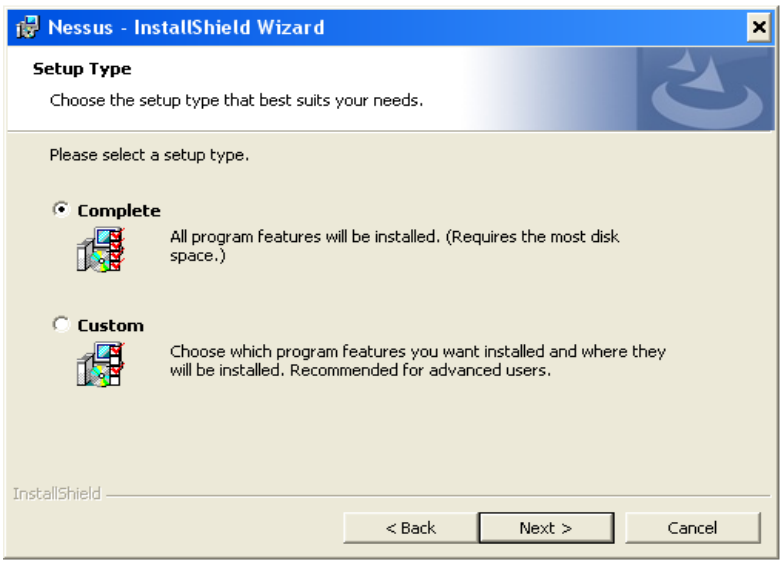
Nessus - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Tenable Network Security, Inc.
NESSUS®
software license Agreement
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers your permitted use of the Software.
BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

Danach können Sie den Installationsort von Nessus konfigurieren:

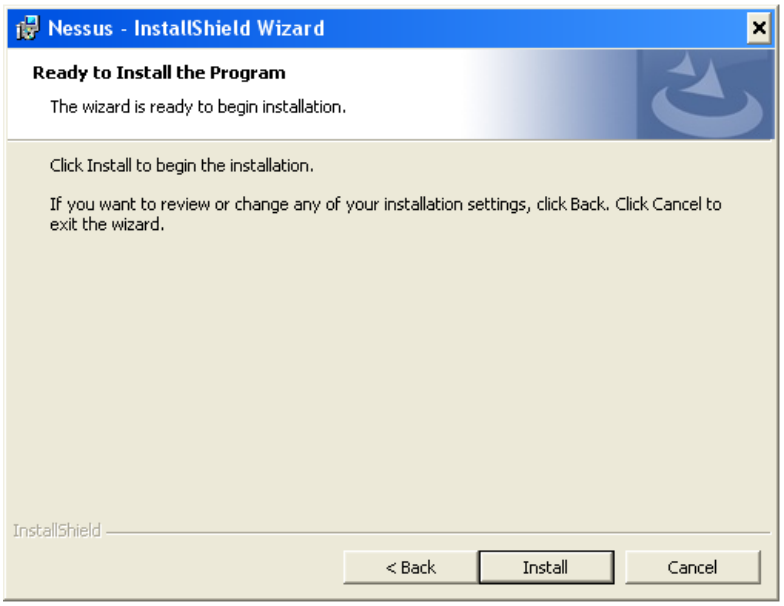


Wenn Sie zur Auswahl von „Setup Type" („Setuptyp") aufgefordert werden, wählen Sie „Complete" („Vollständig").

Copyright © 2002-2011 Tenable Network Security, Inc.

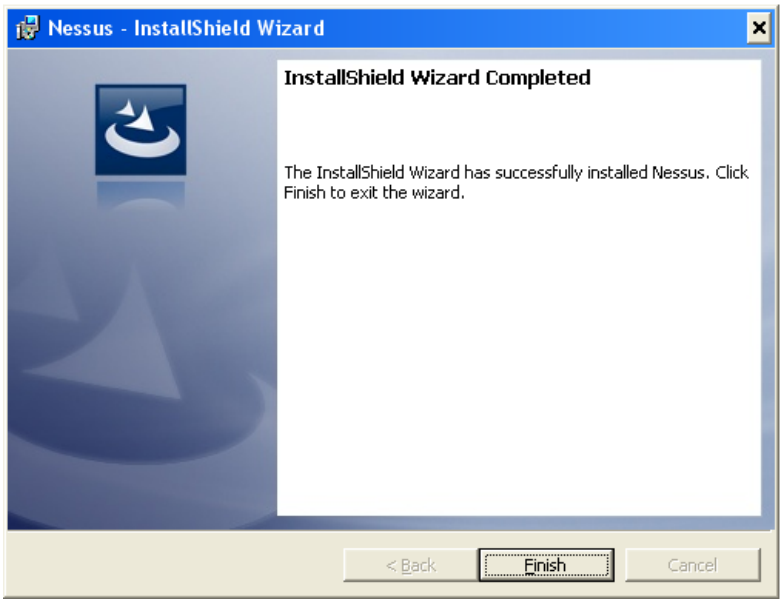

Nessus - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

Sie werden nun aufgefordert, die Installation zu bestätigen:


Nessus - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

Klicken Sie nach Abschluss der Installation auf „Finish“ („Fertig stellen“).

Copyright © 2002-2011 Tenable Network Security, Inc.


Nessus - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Nessus. Click Finish to exit the wizard.
< Back
Finish
Cancel

Die wichtigsten Nessus-Verzeichnisse

Nessus-Stammverzeichnis	Nessus-Unterverzeichnisse	Zweck
Windows		
\Program Files\Tenable\Nessus	**\conf**	Konfigurationsdateien
	\data	Stylesheetvorlagen
	\nessus\plugins	Nessus-Plugins
	\nessus\users\<username>\kbs	Auf Festplatte gespeicherte User-Knowledge-Base
	\nessus\logs	Nessus-Logdateien

Wenn der für die Protokolle erforderliche Festplattenspeicher sich außerhalb des **/opt**-Dateisystems befindet, stellen Sie das gewünschte Zielverzeichnis mithilfe des Befehls „**mount --bind <olddir> <newdir>**" bzw. der für Ihre Distribution passenden Syntax bereit. Symbolische Verknüpfungen dürfen zu diesem Zweck nicht eingesetzt werden.

KONFIGURATION

Dieser Abschnitt beschreibt, wie Sie den Nessus 4-Server auf einem Windows-System konfigurieren.

Nessus Server Manager

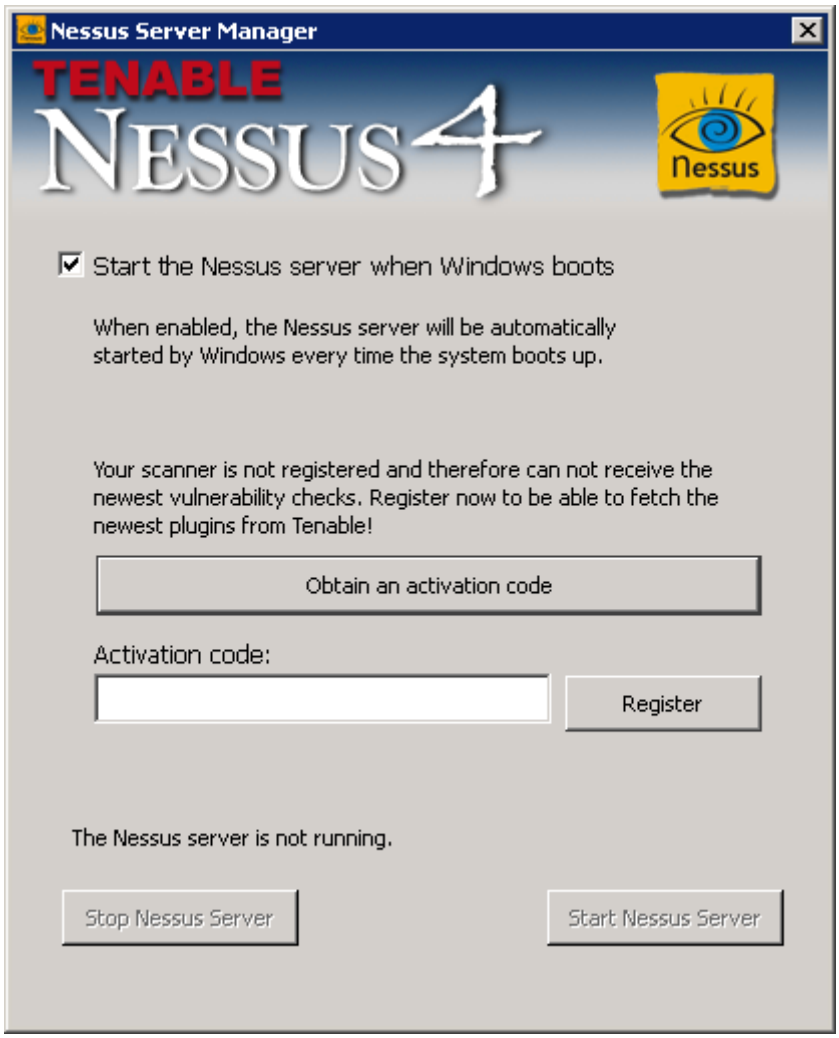
Mit dem Nessus Server Manager können Sie den Nessus-Server starten, beenden und konfigurieren.

Copyright © 2002-2011 Tenable Network Security, Inc.

Über diese Benutzeroberfläche können Sie

- Ihren Nessus-Server auf nessus.org registrieren, um aktualisierte Plugins zu empfangen,
- ein Plugin-Update ausführen,
- einstellen, ob der Nessus-Server bei jedem Windows-Start automatisch gestartet wird,
- Nessus-Benutzer verwalten,
- den Nessus-Server starten und beenden.

Navigieren Sie wie folgt über das Startmenü zum Nessus Server Manager: **Start** -> **Programme** -> **Tenable Network Security** -> **Nessus** -> **Nessus Server Manager**. Nun wird der Nessus Server Manager (`nessussvrmanager.exe`) wie nachfolgend abgebildet gestartet:


Nessus Server Manager
TENABLE
NESSUS 4
Nessus
Start the Nessus server when Windows boots
When enabled, the Nessus server will be automatically started by Windows every time the system boots up.
Your scanner is not registered and therefore can not receive the newest vulnerability checks. Register now to be able to fetch the newest plugins from Tenable!
Obtain an activation code
Activation code:
Register
The Nessus server is not running.
Stop Nessus Server
Start Nessus Server

Die Schaltfläche „Start Nessus Server“ („Nessus-Server starten“) kann erst bedient werden, nachdem die Registrierung des Nessus-Servers erfolgreich durchgeführt wurde.

Copyright © 2002-2011 Tenable Network Security, Inc.

Den Nessus-Standardport ändern

Zur Änderung des Ports, auf dem der Nessus-Server horcht, bearbeiten Sie die Datei **nessusd.conf** im Verzeichnis **C:\Program Files\Tenable\Nessus\conf**. Die folgenden Konfigurationsanweisungen können bearbeitet werden, um die Voreinstellungen für den Listener des Nessus-Diensts und den Webserver zu ändern:

```
# Port to listen to (old NTP protocol). Used for pre 4.2 NessusClient
# connections :
listen_port = 1241

# Port for the Nessus Web Server to listen to (new XMLRPC protocol) :
xmlrpc_listen_port = 8834
```

Nachdem Sie diese Einstellungen geändert haben, beenden Sie über den Nessus Server Manager den Nessus-Dienst und starten ihn dann neu.

Die herkömmliche Clientnutzung über das NTP-Protokoll steht nur ProfessionalFeed-Kunden zur Verfügung.

Nessus-Installation registrieren

Wenn Sie Tenable SecurityCenter verwenden, werden der Aktivierungscode und Plugin-Updates über SecurityCenter verwaltet. Zur Kommunikation mit SecurityCenter muss Nessus gestartet werden, was gewöhnlich ohne einen gültigen Aktivierungscode und Plugins nicht möglich ist. Damit diese Anforderung von Nessus ignoriert wird und ein Start erfolgen kann (und die Informationen aus SecurityCenter abgerufen werden können), führen Sie in der MS-DOS-Eingabeaufforderung folgenden Befehl aus:

```
C:\Program Files\Tenable\Nessus>nessus-fetch --security-center
```

Verwenden Sie unmittelbar nach Ausführung des obigen Befehls „**nessus-fetch**" zum Start des Nessus-Servers den Windows-Dienst-Manager. Der Nessus-Server kann SecurityCenter nun über die SecurityCenter-Weboberfläche hinzugefügt werden. Informationen zur Konfiguration eines zentralen Plugin-Feeds für mehrere Nessus-Scanner finden Sie in der SecurityCenter-Dokumentation.

Nach der Installation müssen Sie Ihren Nessus-Server zunächst registrieren. Erst nach der Registrierung können Sie auf die neuesten Plugins von nessus.org zugreifen und so sicherstellen, dass Ihre Audits auf dem aktuellen Stand sind.

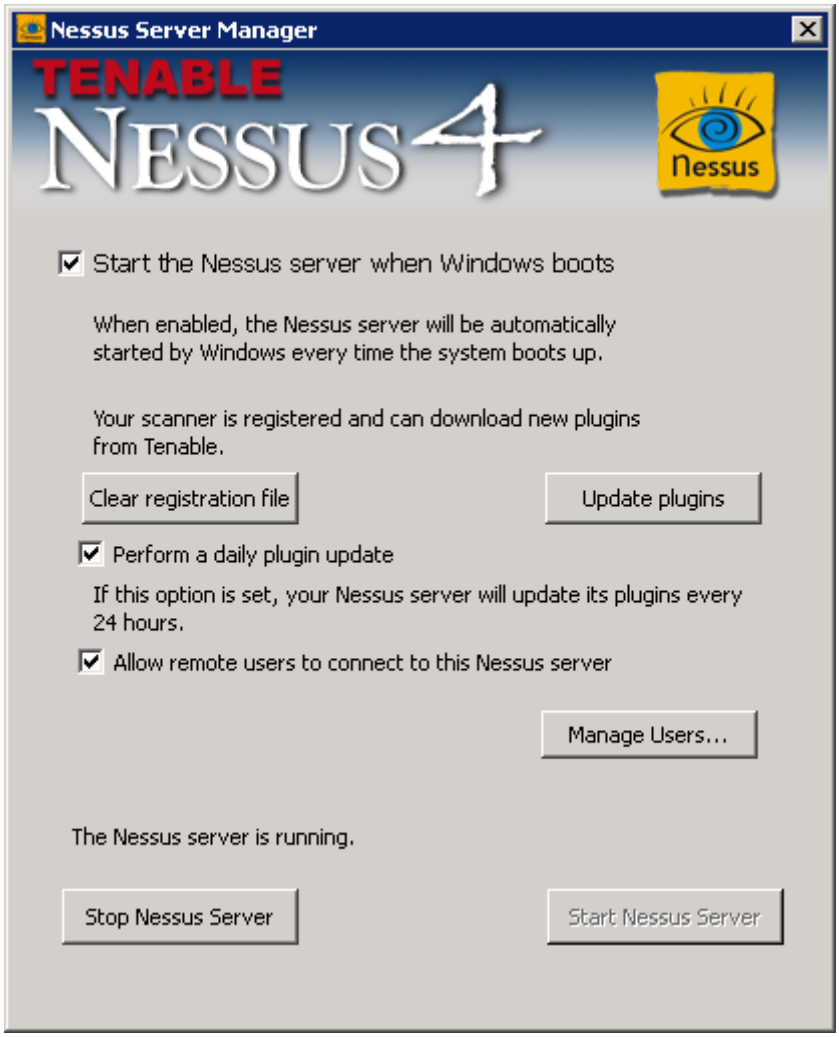
Nach der erstmaligen Registrierung lädt Nessus die Plugins von plugins.nessus.org im Hintergrund herunter und kompiliert sie. Wenn dieser Vorgang zum ersten Mal ausgeführt wird, kann es bis zu zehn Minuten dauern, bis der Nessus-Server betriebsbereit ist. Die Webserveroberfläche ist erst verfügbar, nachdem die Plugins heruntergeladen und kompiliert wurden. Beim Aktivierungscode braucht die Groß-/Kleinschreibung **nicht** beachtet werden.

Copyright © 2002-2011 Tenable Network Security, Inc.

Klicken Sie zur Registrierung von Nessus auf „Obtain an Activation Code" („Aktivierungscode beziehen"). Die Webadresse http://www.nessus.org/plugins/?view=register-info wird aufgerufen. Dort können Sie wahlweise den ProfessionalFeed oder den HomeFeed bestellen. Ein ProfessionalFeed ist für die kommerzielle Nutzung erforderlich und bietet Plugin-Updates, Kundensupport, Konfigurationsaudits, Virtualisierungsfunktionen und mehr. Ein HomeFeed ist für Privatbenutzer vorgesehen und darf nicht beruflich oder kommerziell genutzt werden. Nach der Übermittlung und Verarbeitung der erforderlichen Angaben erhalten Sie eine E-Mail mit dem Aktivierungscode, mit dem Sie entweder den ProfessionalFeed oder den HomeFeed der Plugins beziehen können. Geben Sie den Code in das passende Feld ein und klicken Sie auf die Schaltfläche „Register" („Registrieren"). Beachten Sie, dass Sie aufgefordert werden, Benutzernamen und Kennwort des Administrators einzugeben. Sobald der Nessus Server Manager den Feedaktivierungscode autorisiert, startet das Update der Nessus-Plugins. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen, da der erstmalige Plugin-Download sehr umfangreich ist.

Wenn Sie Ihre Nessus-Kopie nicht registrieren, können Sie weder neue Plugins beziehen noch den Nessus-Server starten.

Nach der Registrierung zeigt der Nessus Server Manager Folgendes an:


Nessus Server Manager
TENABLE
NESSUS 4
Nessus
Start the Nessus server when Windows boots
When enabled, the Nessus server will be automatically started by Windows every time the system boots up.
Your scanner is registered and can download new plugins from Tenable.
Clear registration file
Update plugins
Perform a daily plugin update
If this option is set, your Nessus server will update its plugins every 24 hours.
Allow remote users to connect to this Nessus server
Manage Users...
The Nessus server is running.
Stop Nessus Server
Start Nessus Server

Copyright © 2002-2011 Tenable Network Security, Inc.

Hinweis: Nessus kann auch über die Befehlszeile gestartet werden:

```
C:\Windows\system32>net stop "Tenable Nessus"
The Tenable Nessus service is stopping.
The Tenable Nessus service was stopped successfully.


C:\Windows\system32>net start "Tenable Nessus"
The Tenable Nessus service is starting.
The Tenable Nessus service was started successfully.


C:\Windows\system32>
```

Aktivierungscodes zurücksetzen

Unter bestimmten Umständen – beispielsweise bei einem Upgrade vom HomeFeed auf einen ProfessionalFeed – kann es erforderlich sein, den Aktivierungscode zu wechseln. Hierzu steht die Schaltfläche „Clear Registration File" („Registrierungsdatei löschen") im Nessus Server Manager zur Verfügung. Nach Anklicken der Schaltfläche und Bestätigung des Vorgangs wird die Registrierung Ihrer Nessus-Kopie aufgehoben, bis ein neuer Aktivierungscode eingegeben und das Produkt erneut registriert wird.

Nessus-Benutzer erstellen und verwalten

Remoteverbindungen zulassen

Wenn Sie einen Remotebetrieb des Nessus-Scanners beabsichtigen (beispielsweise in Verbindung mit SecurityCenter), müssen Sie das Kontrollkästchen „**Allow remote users to connect to this Nessus server**" („Remotebenutzern die Verbindung mit diesem Nessus-Server gestatten") aktivieren.

Wenn das Kontrollkästchen nicht aktiviert ist, steht der Nessus-Server nur lokalen Clients zur Verfügung.

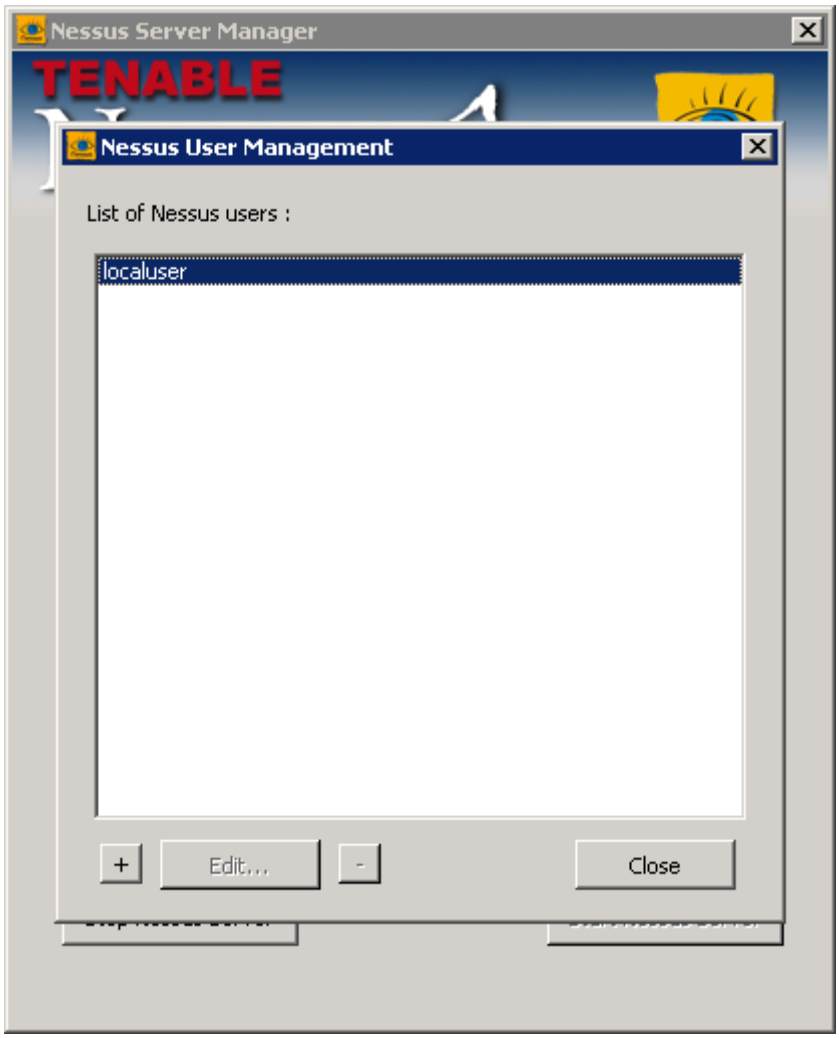
Ist das Kontrollkästchen hingegen aktiviert, dann kann der Zugriff auf den Nessus-Server über Clients, die wahlweise auf dem lokalen oder einem Remotehost installiert sind, wie auch über die SecurityCenter-Oberfläche erfolgen (diese wird weiter unten im Abschnitt „Mit SecurityCenter arbeiten" beschrieben).

Informationen zu Nessus-Clients entnehmen Sie dem „Nessus 4.4 Benutzerhandbuch".

Benutzerkonten hinzufügen

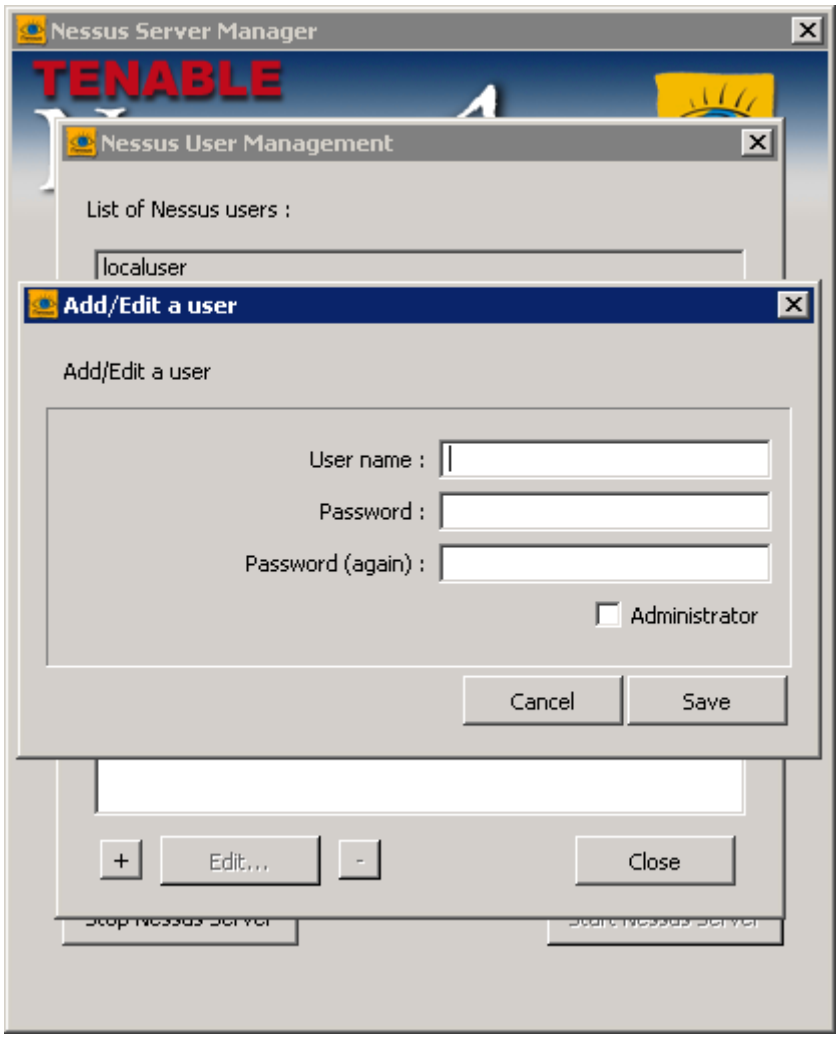
Nach einem Klick auf „Manage Users…" („Benutzer verwalten…") können Sie Konten für den Nessus-Server erstellen und verwalten:

Copyright © 2002-2011 Tenable Network Security, Inc.



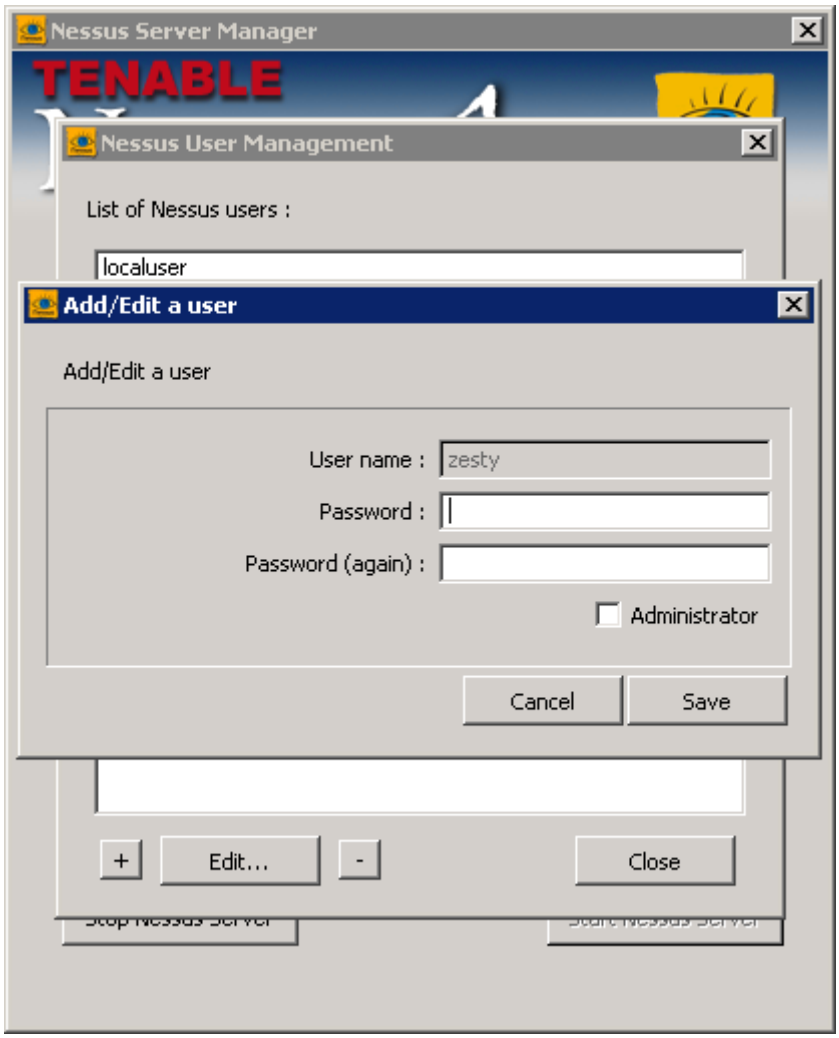
Klicken Sie zur Erstellung eines Benutzers auf die Schaltfläche „+" und geben nachfolgend einen neuen Benutzernamen und ein Kennwort ein. Aktivieren Sie das Kontrollkästchen „Administrator", wenn es sich bei diesem Benutzer um einen Administrator handeln soll:

Copyright © 2002-2011 Tenable Network Security, Inc.



Nach Auswahl eines Namens auf der Liste und Anklicken der Schaltfläche „Edit…" („Bearbeiten") können Sie das Kennwort des Benutzers ändern (siehe nachfolgende Abbildung). Wenn Sie auf die Schaltfläche „–" klicken, wird der Benutzer nach Bestätigung gelöscht.

Copyright © 2002-2011 Tenable Network Security, Inc.



Sie können einen Benutzer nicht umbenennen. Wenn Sie den Namen eines Benutzers ändern möchten, müssen Sie den Benutzer löschen und dann einen neuen Benutzer mit dem passenden Anmeldenamen erstellen.

Beachten Sie, dass Nessus ein internes Verwaltungskonto für die lokale Kommunikation zwischen der Nessus-Benutzeroberfläche und dem Tenable Nessus Service verwendet. Dieses Konto kann nicht für Remoteverbindungen mit einem Nessus-Client verwendet werden.

Hostbasierte Firewalls

Wenn Ihr Nessus-Server auf einem Host mit einer Personal Firewall wie beispielsweise Zone Alarm, Sygate, der Windows XP-Firewall oder einer anderen Firewallsoftware konfiguriert ist, müssen Verbindungsanfragen von der IP-Adresse des Nessus-Clients zugelassen werden.

Standardmäßig wird für den Nessus Web Server (d. h. die Benutzeroberfläche) Port 8834 verwendet. Auf Systemen unter Microsoft XP Service Pack 2 (SP2) und höher erhält der Benutzer nach dem Klick auf das „**Sicherheitscenter**" in der „**Systemsteuerung**" die

Copyright © 2002-2011 Tenable Network Security, Inc.

Möglichkeit, die Einstellungen der Windows-Firewall zu verwalten. Um Port 8834 zu öffnen, wählen Sie die Registerkarte „**Ausnahmen**" aus und fügen Sie der Liste Port 8834 hinzu.

Ziehen Sie im Falle anderer Personal Firewalls die Dokumentation zurate, um diese Konfiguration durchzuführen.

Den Nessus-Daemon starten

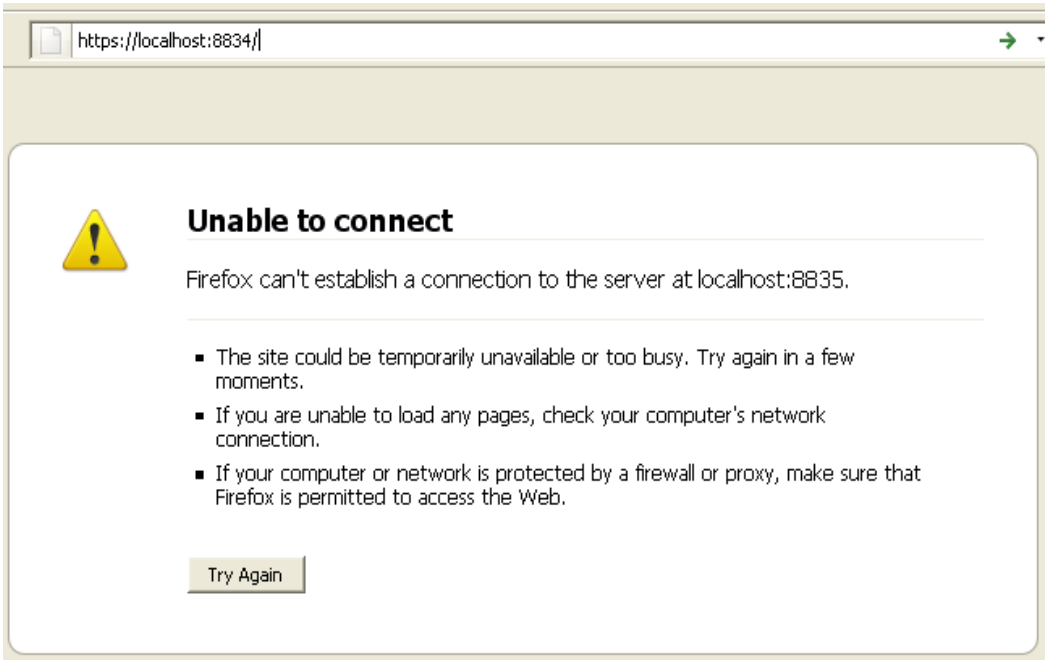
Klicken Sie zum Starten des Nessus-Daemons im Nessus Server Manager auf die Schaltfläche „**Start Nessus Server**" („Nessus-Server starten").

Wenn Nessus jeweils automatisch gestartet werden soll, aktivieren Sie das Kontrollkästchen „**Start the Nessus Server when Windows boots**" („Nessus-Server beim Windows-Start automatisch starten").

Nessus wird unter Windows als Dienst „Tenable Nessus" installiert und für den automatischen Start beim Systemneustart konfiguriert. Diese Einstellung wird mithilfe des Kontrollkästchens „Start the Nessus Server when Windows boots" konfiguriert.

Nach Start des Dienstes **`nessusd`** ist die Erstinstallation und -konfiguration des Nessus 4-Scanners für SecurityCenter-Benutzer abgeschlossen. Diese können nun mit dem Abschnitt „Mit SecurityCenter arbeiten" fortfahren.

Wenn der Nessus-Daemon nicht ausgeführt wird oder die Benutzeroberfläche nicht vorhanden ist, erscheint in Ihrem Webbrowser eine Fehlermeldung, die besagt, dass keine Verbindung hergestellt werden kann:


https://localhost:8834/
Unable to connect
Firefox can't establish a connection to the server at localhost:8835.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again

Der Nessus-Server wird auf „localhost" (127.0.0.1) ausgeführt und horcht standardmäßig auf Port 1241 nach herkömmlichen Clients. Wenn Sie überprüfen möchten, dass Nessus auf

Copyright © 2002-2011 Tenable Network Security, Inc.

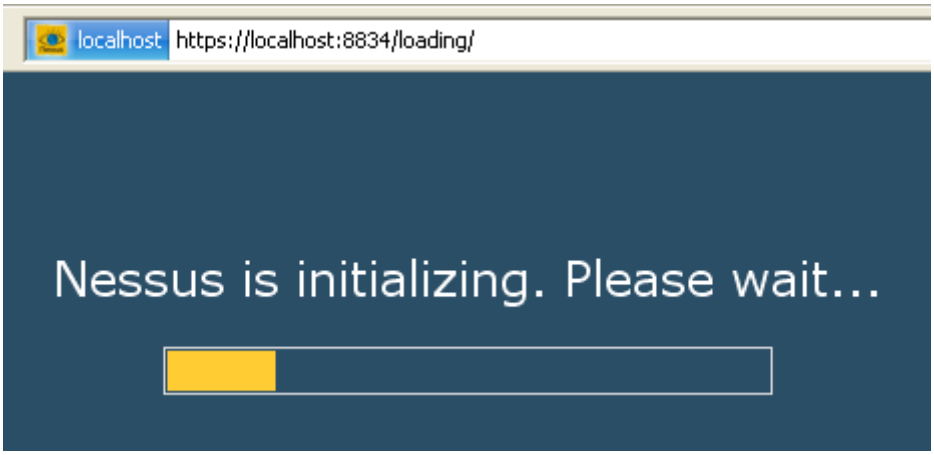
Port 1241 horcht, verwenden Sie wie nachfolgend gezeigt den Befehl „**`netstat -an | findstr 1241`**“ in der Windows-Befehlszeile:

```
C:\Documents and Settings\admin>netstat -an | findstr 1241
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
```

Achten Sie darauf, dass die Ausgabe „0.0.0.0:1241” enthält; dies ist ein Hinweis darauf, dass ein Server auf diesem Port horcht. Mithilfe dieser Angabe kann auch überprüft werden, ob der Webserver (Benutzeroberfläche) verfügbar ist. Dazu ersetzen Sie im obigen Befehl einfach „1241“ durch „8834“.

Beachten Sie, dass der automatische Start des Nessus-Diensts erst erfolgen kann, wenn die Installation abgeschlossen wurde **und** ein Plugin-Update stattgefunden hat.

Die erstmalige Aktualisierung und Verarbeitung der Plugins durch Nessus kann mehrere Minuten in Anspruch nehmen. Der Webserver zeigt die Meldung „Nessus is initializing“ („Nessus wird initialisiert“) an und wird nach Abschluss des Vorgangs neu geladen:



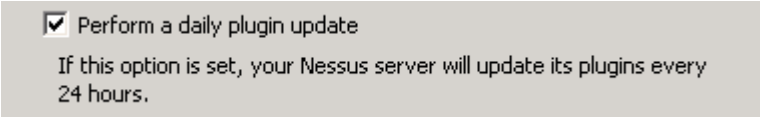
Wenn Sie erstmals eine Verbindung mit der Weboberfläche herstellen, zeigt Ihr Browser möglicherweise einen Warnhinweis zu einer nicht vertrauenswürdigen Verbindung an. Dies liegt daran, dass Nessus im Auslieferungszustand ein SSL-Standardzertifikat nutzt. Weitere Informationen hierzu entnehmen Sie dem Nessus-Benutzerhandbuch.

Plugin-Updates ausführen

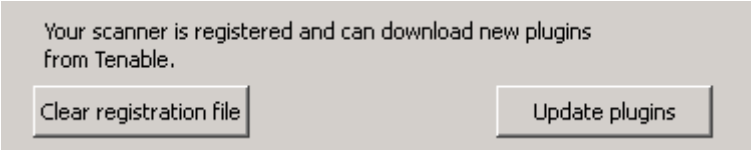
Nessus umfasst Zehntausende von Plugins (oder Skripts), die Tests auf Schwachstellen im Netzwerk und auf Hosts ausführen. Regelmäßig werden neue Sicherheitslücken gefunden, und neue Plugins werden entwickelt, um diese Sicherheitslücken zu erkennen. Damit Ihr Nessus-Scanner auf dem aktuellen Stand bleibt und stets die neuesten Plugins benutzt, müssen Sie Ihre Plugins täglich aktualisieren, denn nur so kann der Scanner zuverlässig arbeiten.

Mit der Option „**Perform a daily plugin update**“ („Plugin-Update täglich ausführen“) wird der Nessus-Server automatisch so konfiguriert, dass alle 24 Stunden Plugin-Updates von Tenable abgerufen werden. Dieser Vorgang erfolgt ungefähr zu der Uhrzeit, zu der Sie Nessus gestartet haben.

Copyright © 2002-2011 Tenable Network Security, Inc.



Sie können ein Plugin-Update auch erzwingen. Klicken Sie dazu auf die Schaltfläche „**Update Plugins**" („Plugins aktualisieren"):



Wie oft soll ich meine Plugins aktualisieren?

Im Allgemeinen ist eine tägliche Aktualisierung der Nessus-Plugins für die meisten Organisationen ausreichend. Wenn Sie jedoch stets die aktuellsten Plugins benötigen und eine fortlaufende Aktualisierung während des gesamten Tages wünschen, können Sie in einem 4-Stunden-Turnus Aktualisierungen durchführen. Eine häufigere Aktualisierung bringt praktisch keinen zusätzlichen Nutzen.

Plugins über Webproxys aktualisieren

Unter Windows unterstützt Nessus die Produktregistrierung und Plugin-Updates über Webproxys, die eine Standardauthentifizierung erfordern. Die Proxyeinstellungen finden Sie in der Datei **`C:\Program Files\Tenable\Nessus\conf\nessus-fetch.rc`**. Vier Zeilen sind für die Steuerung proxybasierter Verbindungen relevant. Sie sind nachfolgend mit einer Beispielsyntax aufgeführt:

```
proxy=myproxy.example.com
proxy_port=8080
proxy_username=juser
proxy_password=guineapig
```

Für die Anweisung „**`proxy`**" können ein DNS-Hostname oder eine IP-Adresse verwendet werden. In der Datei **`nessus-fetch.rc`** darf nur ein Proxy angegeben sein. Zusätzlich kann erforderlichenfalls eine **`user_agent`** Anweisung angegeben werden, die die Verwendung eines benutzerdefinierten HTTP-Benutzeragenten in Nessus erzwingt.

Seit Nessus 4.2 unterstützen Microsoft Windows-Scanner die Proxyauthentifizierung einschließlich NTLM.

NESSUS ENTFERNEN

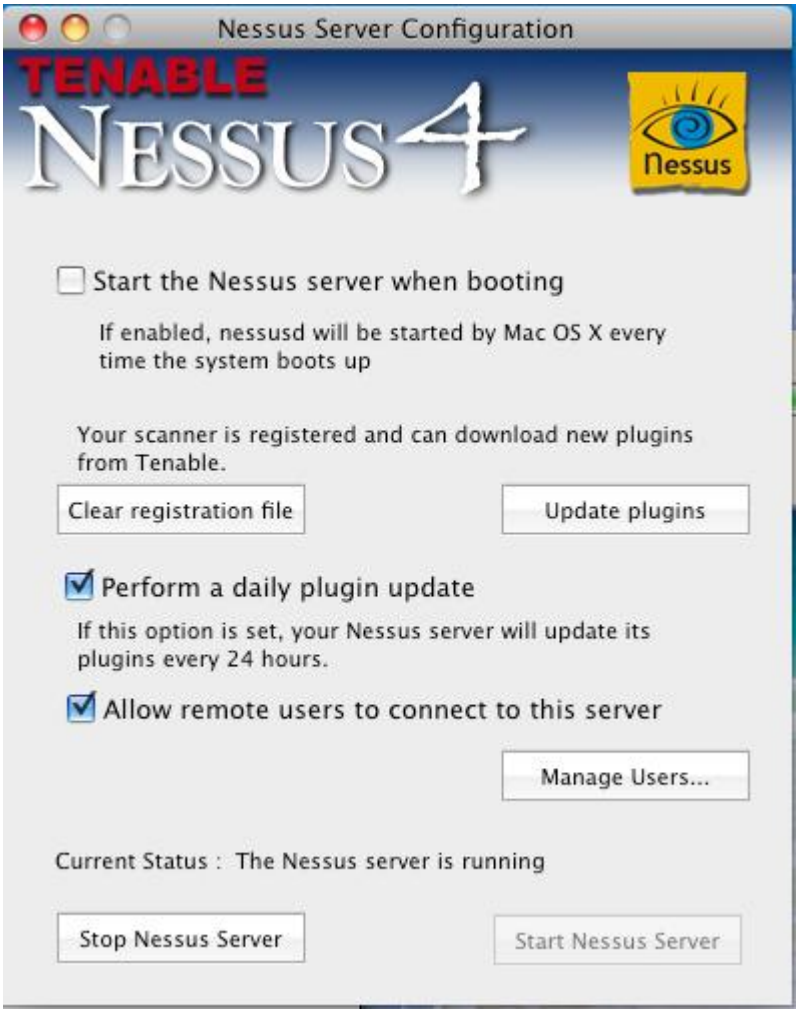
Rufen Sie in der Systemsteuerung den Eintrag „**Software**" auf, um Nessus zu entfernen. Wählen Sie „**Tenable Nessus**" aus und klicken Sie dann auf die Schaltfläche „**Ändern/Entfernen**". Das Fenster InstallShield Wizard wird geöffnet. Befolgen Sie die Anweisungen im Assistenten, um Nessus vollständig zu entfernen. Sie werden aufgefordert, festzulegen, ob Sie den gesamten Nessus-Ordner entfernen möchten. Wählen Sie „Yes" nur dann aus, wenn Sie keine zuvor generierten Scanergebnisse und -richtlinien behalten möchten.

Copyright © 2002-2011 Tenable Network Security, Inc.

MAC OS X

UPGRADE AUSFÜHREN

Das Upgrade von einer älteren Nessus-Version ähnelt der Neuinstallation. Allerdings müssen Sie den Nessus-Server am Ende der Installation beenden und neu starten. Laden Sie die Datei **`Nessus-4.x.x.dmg.gz`** herunter und doppelklicken Sie darauf, um sie zu entpacken. Doppelklicken Sie dann auf die Datei **`Nessus-4.x.x.dmg`**. Mithilfe dieser Datei wird das Image aktiviert und unter „Geräte" im Finder aufgeführt. Sobald das Volume „Nessus 4" im Finder angezeigt wird, doppelklicken Sie auf die Datei **`Nessus 4`**. Navigieren Sie nach Abschluss der Installation zu **`/Applications/Nessus/`** und führen den Nessus Server Manager aus. Zum Abschluss des Upgrades müssen Sie auf „Update Plugins" („Plugins aktualisieren") klicken:


Nessus Server Configuration
TENABLE
NESSUS 4
Nessus
Start the Nessus server when booting
If enabled, nessusd will be started by Mac OS X every time the system boots up
Your scanner is registered and can download new plugins from Tenable.
Clear registration file
Update plugins
Perform a daily plugin update
If this option is set, your Nessus server will update its plugins every 24 hours.
Allow remote users to connect to this server
Manage Users...
Current Status : The Nessus server is running
Stop Nessus Server
Start Nessus Server

INSTALLATION

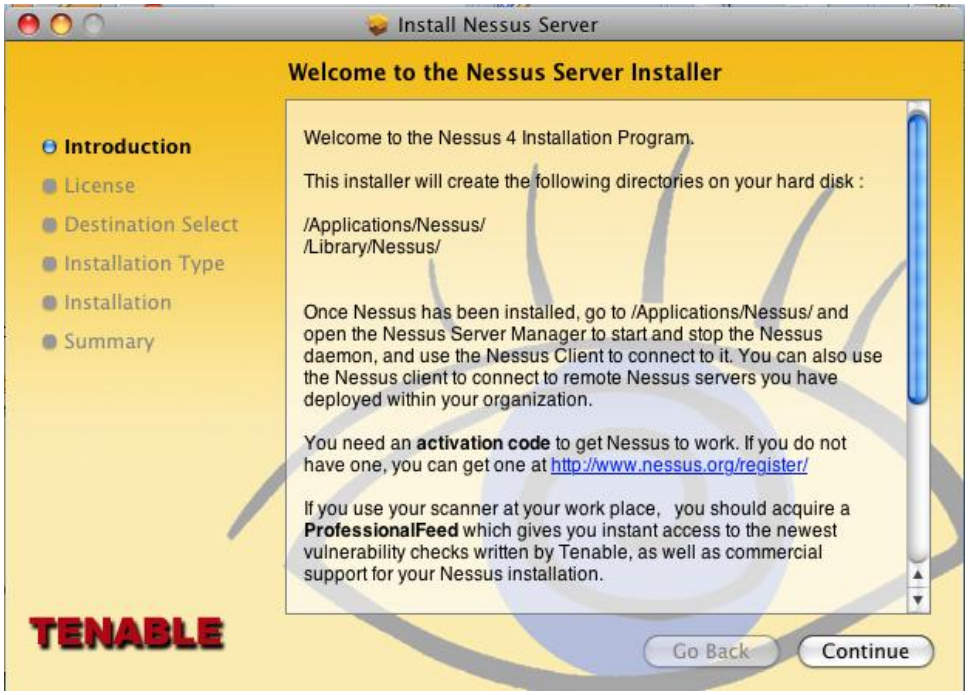
Die aktuellste Version von Nessus steht unter http://www.nessus.org/download/ zum Download bereit. Nessus ist für Mac OS X 10.4 und 10.5 erhältlich. Überprüfen Sie die Integrität des Installationspakets, indem Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei **`MD5.asc`** (hier) angegebenen Prüfsumme vergleichen.

Copyright © 2002-2011 Tenable Network Security, Inc.

Laden Sie zur Installation von Nessus unter Mac OS X die Datei **`Nessus-4.x.x.dmg.gz`** herunter und doppelklicken darauf, um sie zu entpacken. Doppelklicken Sie dann auf die Datei **`Nessus-4.x.x.dmg`**. Mithilfe dieser Datei wird das Image aktiviert und unter „Geräte" im Finder aufgeführt. Sobald das Volume „Nessus 4" im Finder angezeigt wird, doppelklicken Sie wie nachfolgend gezeigt auf die Datei **`Nessus 4`**:

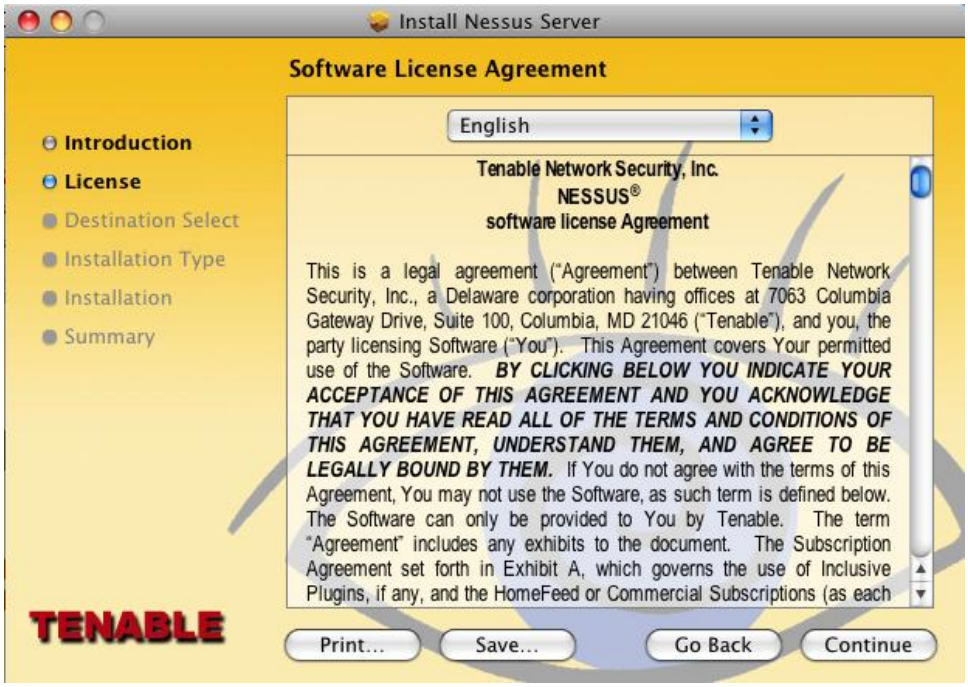
Beachten Sie, dass Sie während der Installation mehrfach zur Eingabe des Administratornamens und Kennworts aufgefordert werden.

Die Installation wird wie folgt angezeigt:

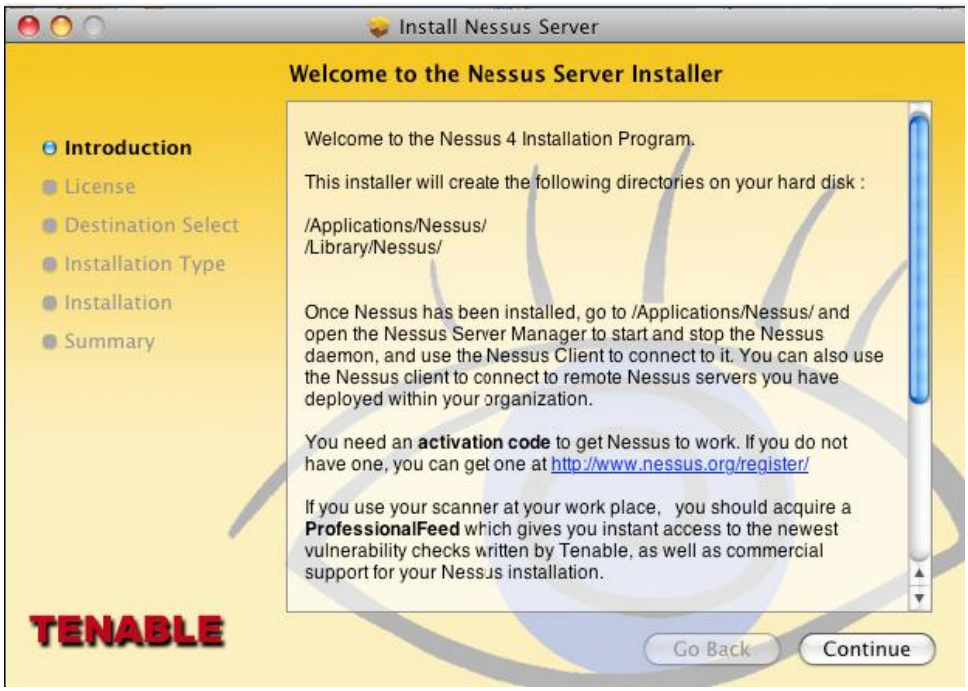

Install Nessus Server
Welcome to the Nessus Server Installer
Introduction
License
Destination Select
Installation Type
Installation
Summary
Welcome to the Nessus 4 Installation Program.
This installer will create the following directories on your hard disk :
/Applications/Nessus/
/Library/Nessus/
Once Nessus has been installed, go to /Applications/Nessus/ and open the Nessus Server Manager to start and stop the Nessus daemon, and use the Nessus Client to connect to it. You can also use the Nessus client to connect to remote Nessus servers you have deployed within your organization.
You need an activation code to get Nessus to work. If you do not have one, you can get one at http://www.nessus.org/register/
If you use your scanner at your work place, you should acquire a ProfessionalFeed which gives you instant access to the newest vulnerability checks written by Tenable, as well as commercial support for your Nessus installation.
TENABLE
Go Back
Continue

Copyright © 2002-2011 Tenable Network Security, Inc.

Klicken Sie auf „Continue" („Weiter"). Es wird ein Dialogfeld angezeigt, in dem Sie die Lizenzbedingungen akzeptieren müssen, um fortfahren zu können:

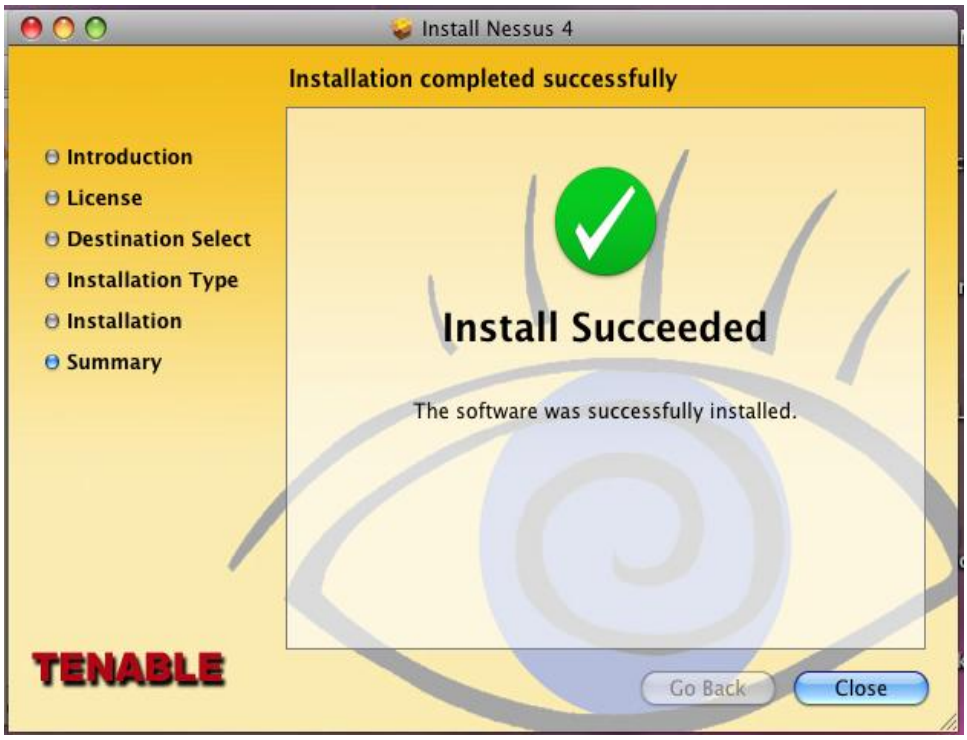

Install Nessus Server
Software License Agreement
Introduction
License
Destination Select
Installation Type
Installation
Summary
English
Tenable Network Security, Inc.
NESSUS®
software license Agreement
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. If You do not agree with the terms of this Agreement, You may not use the Software, as such term is defined below. The Software can only be provided to You by Tenable. The term "Agreement" includes any exhibits to the document. The Subscription Agreement set forth in Exhibit A, which governs the use of Inclusive Plugins, if any, and the HomeFeed or Commercial Subscriptions (as each
TENABLE
Print...
Save...
Go Back
Continue

Nach dem Akzeptieren der Lizenz erscheint ein weiteres Dialogfeld, in dem Sie den vorgegebenen Installationsort wie gezeigt ändern können:


Install Nessus Server
Welcome to the Nessus Server Installer
Introduction
License
Destination Select
Installation Type
Installation
Summary
Welcome to the Nessus 4 Installation Program.
This installer will create the following directories on your hard disk :
/Applications/Nessus/
/Library/Nessus/
Once Nessus has been installed, go to /Applications/Nessus/ and open the Nessus Server Manager to start and stop the Nessus daemon, and use the Nessus Client to connect to it. You can also use the Nessus client to connect to remote Nessus servers you have deployed within your organization.
You need an activation code to get Nessus to work. If you do not have one, you can get one at http://www.nessus.org/register/
If you use your scanner at your work place, you should acquire a ProfessionalFeed which gives you instant access to the newest vulnerability checks written by Tenable, as well as commercial support for your Nessus installation.
TENABLE
Go Back
Continue

Klicken Sie auf „Install" („Installieren"), um die Installation fortzusetzen. Sie werden nun aufgefordert, den Benutzernamen und das Kennwort des Administrators einzugeben. Die Installation wurde erfolgreich abgeschlossen, wenn das folgende Fenster erscheint:

Copyright © 2002-2011 Tenable Network Security, Inc.

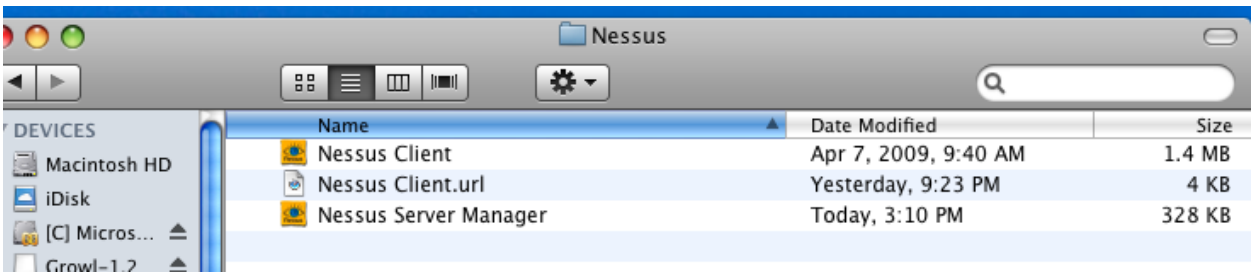


Konfiguration

Dieser Abschnitt beschreibt, wie Sie den Nessus 4-Server auf einem Mac OS X-System konfigurieren.

Nessus Server Manager

Mit dem Programm Nessus Server Manager, das unter **`/Applications/Nessus/`** gespeichert ist, können Sie den Nessus-Server starten, beenden und konfigurieren:



Beachten Sie, dass, wenn Sie Nessus aktualisiert haben, der Nessus Client nach wie vor im Ordner Nessus aufgeführt ist. Sie müssen den Nessus Client nicht mehr zur Verwaltung von Nessus-Scans verwenden, und er kann auf Wunsch entfernt werden. „Nessus Client.url" ist ein Link zur Verwaltung von Nessus in Ihrem Webbrowser. In Neuinstallationen ist der Nessus Client nicht enthalten.

Über die Nessus Server Manager-Oberfläche können Sie

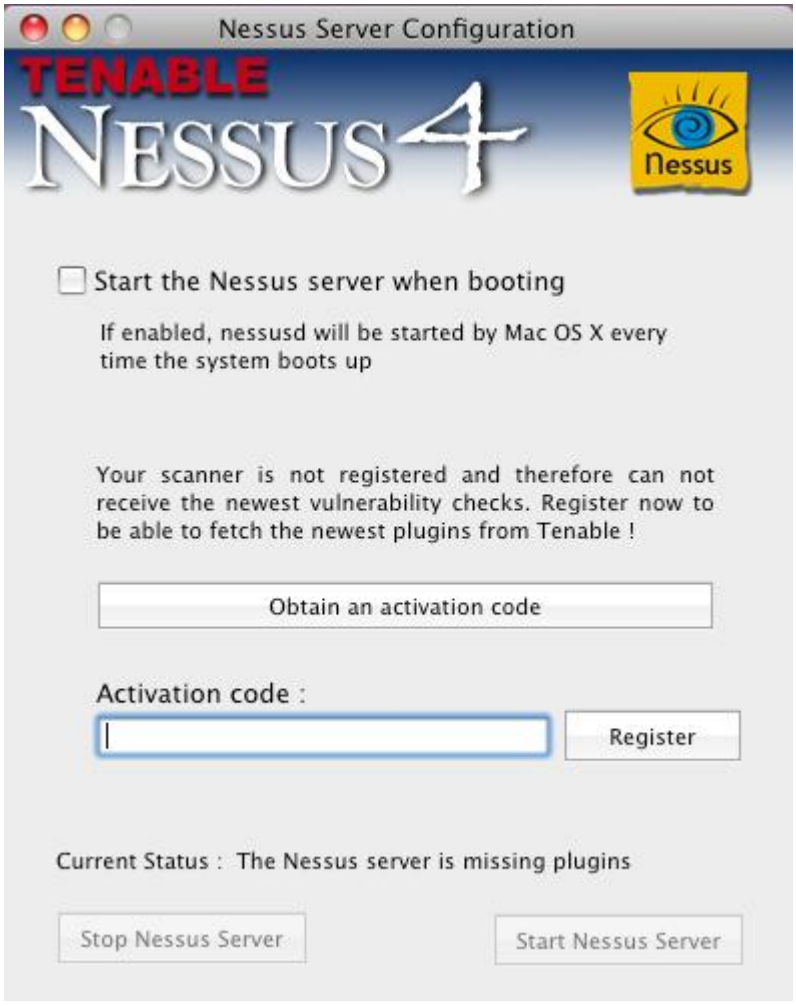
- Ihren Nessus-Server auf nessus.org registrieren, um aktualisierte Plugins zu empfangen,

Copyright © 2002-2011 Tenable Network Security, Inc.

- ein Plugin-Update ausführen,
- einstellen, ob der Nessus-Server bei jedem Mac OS X-Start automatisch gestartet wird,
- Nessus-Benutzer verwalten,
- den Nessus-Server starten und beenden.

Wenn Sie „Nessus Server Manager" starten, werden Sie aufgefordert, den Administratornamen und das Kennwort einzugeben. Dies ist notwendig, weil zur Interaktion mit dem Nessus-Server Root-Zugriffsrechte erforderlich sind.

Doppelklicken Sie zum Start von Nessus Server Manager auf das Symbol. Der folgende Startbildschirm wird angezeigt:


Nessus Server Configuration
TENABLE
NESSUS 4
Nessus
Start the Nessus server when booting
If enabled, nessusd will be started by Mac OS X every time the system boots up
Your scanner is not registered and therefore can not receive the newest vulnerability checks. Register now to be able to fetch the newest plugins from Tenable !
Obtain an activation code
Activation code :
Register
Current Status : The Nessus server is missing plugins
Stop Nessus Server
Start Nessus Server

Die Schaltfläche „Start Nessus Server" („Nessus-Server starten") kann erst bedient werden, nachdem die Registrierung des Nessus-Servers erfolgreich durchgeführt wurde.

Copyright © 2002-2011 Tenable Network Security, Inc.

Nessus-Installation registrieren

Wenn Sie Tenable SecurityCenter verwenden, werden der Aktivierungscode und Plugin-Updates über SecurityCenter verwaltet. Zur Kommunikation mit SecurityCenter muss Nessus gestartet werden, was gewöhnlich ohne einen gültigen Aktivierungscode und Plugins nicht möglich ist. Damit diese Anforderung von Nessus ignoriert wird und ein Start erfolgen kann (und die Informationen aus SecurityCenter abgerufen werden können), führen Sie den folgenden Befehl in einem Root-Shell-Prompt aus:

```
# /Library/Nessus/run/bin/nessus-fetch --security-center
```

Geben Sie unmittelbar nach Ausführung des obigen Befehls „**nessus-fetch**" den zum Start des Nessus-Servers erforderlichen Befehl ein. Der Nessus-Server kann SecurityCenter nun über die SecurityCenter-Weboberfläche hinzugefügt werden. Informationen zur Konfiguration eines zentralen Plugin-Feeds für mehrere Nessus-Scanner finden Sie in der SecurityCenter-Dokumentation.

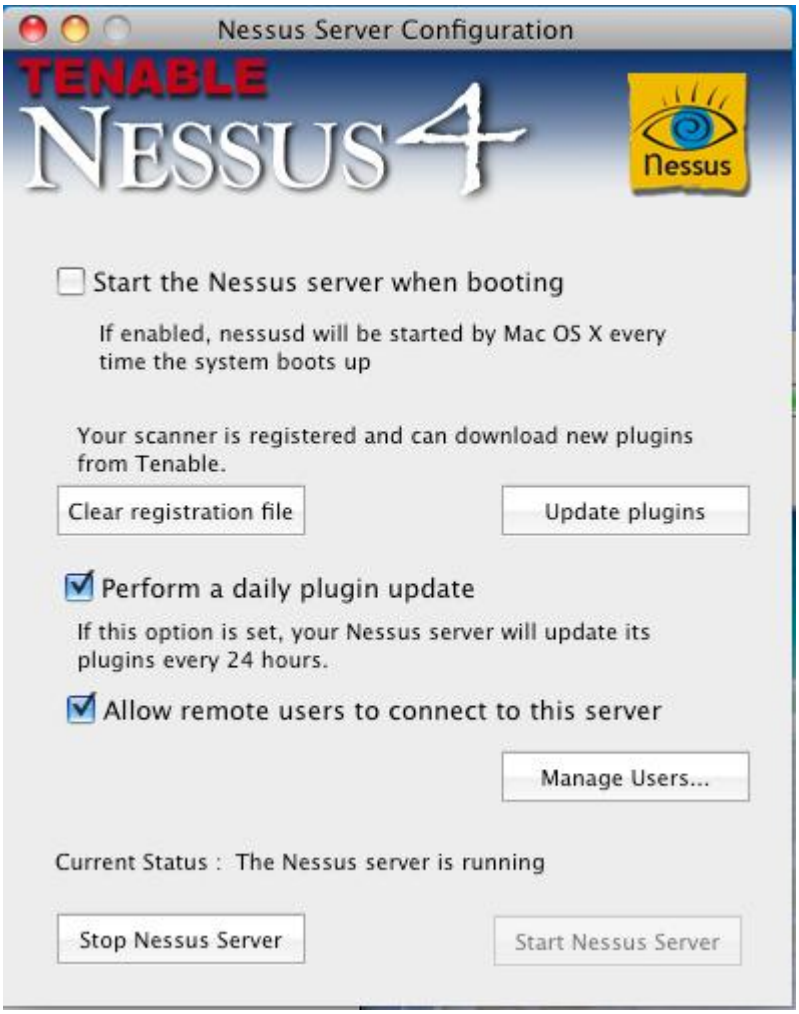
Nach der Installation müssen Sie Ihren Nessus-Server zunächst registrieren. Erst nach der Registrierung können Sie auf die neuesten Plugins von nessus.org zugreifen und so sicherstellen, dass Ihre Audits auf dem aktuellen Stand sind.

Klicken Sie zur Registrierung von Nessus auf „Obtain an Activation Code" („Aktivierungscode beziehen"). Die Webadresse http://www.nessus.org/plugins/?view=register-info wird aufgerufen. Dort können Sie wahlweise den ProfessionalFeed oder den HomeFeed bestellen. Ein ProfessionalFeed ist für die kommerzielle Nutzung erforderlich und bietet Plugin-Updates, Kundensupport, Konfigurationsaudits, Virtualisierungsfunktionen und mehr. Ein HomeFeed ist für Privatbenutzer vorgesehen und darf nicht beruflich oder kommerziell genutzt werden. Nach der Übermittlung und Verarbeitung der erforderlichen Angaben erhalten Sie eine E-Mail mit dem Aktivierungscode, mit dem Sie entweder den ProfessionalFeed oder den HomeFeed der Plugins beziehen können. Geben Sie den Code in das passende Feld ein und klicken Sie auf die Schaltfläche „Register" („Registrieren"). Beachten Sie, dass Sie aufgefordert werden, Benutzernamen und Kennwort des Administrators einzugeben. Sobald der Nessus Server Manager den Feedaktivierungscode autorisiert, startet das Update der Nessus-Plugins. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen, da der erstmalige Plugin-Download sehr umfangreich ist.

Wenn Sie Ihre Nessus-Kopie nicht registrieren, können Sie weder neue Plugins beziehen noch den Nessus-Server starten.

Copyright © 2002-2011 Tenable Network Security, Inc.

Nach der Registrierung zeigt der Nessus Server Manager Folgendes an:


Nessus Server Configuration
TENABLE
NESSUS 4
Nessus
Start the Nessus server when booting
If enabled, nessusd will be started by Mac OS X every time the system boots up
Your scanner is registered and can download new plugins from Tenable.
Clear registration file
Update plugins
Perform a daily plugin update
If this option is set, your Nessus server will update its plugins every 24 hours.
Allow remote users to connect to this server
Manage Users...
Current Status : The Nessus server is running
Stop Nessus Server
Start Nessus Server

Aktivierungscodes zurücksetzen

Unter bestimmten Umständen – beispielsweise bei einem Upgrade vom HomeFeed auf einen ProfessionalFeed – kann es erforderlich sein, den Aktivierungscode zu wechseln. Hierzu steht die Schaltfläche „Clear Registration File" („Registrierungsdatei löschen") im Nessus Server Manager zur Verfügung. Nach Anklicken der Schaltfläche und Bestätigung des Vorgangs wird die Registrierung Ihrer Nessus-Kopie aufgehoben, bis ein neuer Aktivierungscode eingegeben und das Produkt erneut registriert wird.

Nessus-Benutzer erstellen und verwalten

Remoteverbindungen zulassen

Wenn Sie einen Remotebetrieb des Nessus-Scanners beabsichtigen (beispielsweise in Verbindung mit SecurityCenter), müssen Sie das Kontrollkästchen „**Allow remote users to connect to this Nessus server**" („Remotebenutzern die Verbindung mit diesem Nessus-Server gestatten") aktivieren.

Wenn das Kontrollkästchen nicht aktiviert ist, steht der Nessus-Server nur dem lokalen Nessus-Client zur Verfügung.

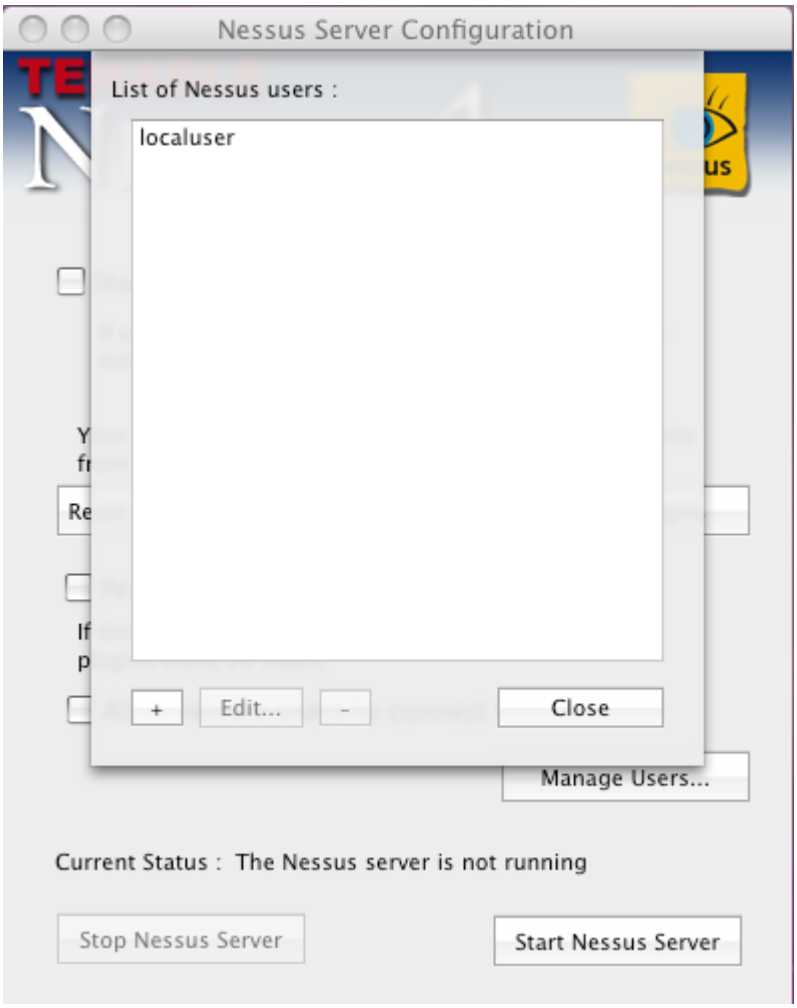
Copyright © 2002-2011 Tenable Network Security, Inc.

Ist das Kontrollkästchen hingegen aktiviert, dann kann der Zugriff auf den Nessus-Server über Clients, die wahlweise auf dem lokalen oder einem Remotehost installiert sind, wie auch über die SecurityCenter-Oberfläche erfolgen (diese wird weiter unten im Abschnitt „Mit SecurityCenter arbeiten" beschrieben).

Informationen zu Nessus-Clients entnehmen Sie dem „Nessus 4.4 Benutzerhandbuch".

Benutzerkonten hinzufügen

Nach einem Klick auf „Manage Users…" („Benutzer verwalten…") können Sie Konten für den Nessus-Server erstellen und verwalten:



Sofern Sie nicht über die erforderliche Erfahrung verfügen, sollten Sie den Benutzer „localuser" nicht löschen, da hierdurch der **`Local Connection`**-Server für Nessus unbrauchbar wird.

Klicken Sie zur Erstellung eines Benutzers auf die Schaltfläche „+" und geben Sie dann einen neuen Benutzernamen und ein Kennwort ein. Aktivieren Sie das Kontrollkästchen „Administrator", wenn es sich bei diesem Benutzer um einen Administrator handeln soll. Nach Auswahl eines Namens aus der Liste und Anklicken der Schaltfläche „Edit…" („Bearbeiten")

Copyright © 2002-2011 Tenable Network Security, Inc.

können Sie das Kennwort des Benutzers ändern (siehe nachfolgende Abbildung). Wenn Sie auf die Schaltfläche „–" klicken, wird der Benutzer nach Bestätigung gelöscht.

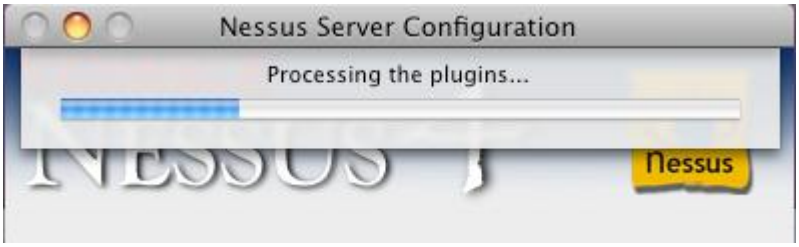
Sie können einen Benutzer nicht umbenennen. Wenn Sie den Namen eines Benutzers ändern möchten, müssen Sie den Benutzer löschen und dann einen neuen Benutzer mit dem passenden Anmeldenamen erstellen.

Den Nessus-Daemon starten

Klicken Sie zum Start des Nessus-Daemons im Nessus Server Manager auf die Schaltfläche „**Start Nessus Server**" („Nessus-Server starten").

Wenn Nessus automatisch gestartet werden soll, aktivieren Sie das Kontrollkästchen „**Start the Nessus Server at bootup**" („Nessus-Server beim Systemstart automatisch starten").

Nach dem Start des **nessusd**-Diensts dauert es einige Minuten, bis die Plugins verarbeitet sind:

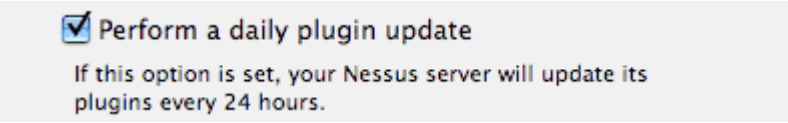


Nach dem Start des Dienstes **nessusd** ist die Erstinstallation und -konfiguration des Nessus 4-Scanners für SecurityCenter-Benutzer abgeschlossen. Diese können nun mit dem Abschnitt „Mit SecurityCenter arbeiten" fortfahren.

PLUGIN-UPDATES AUSFÜHREN

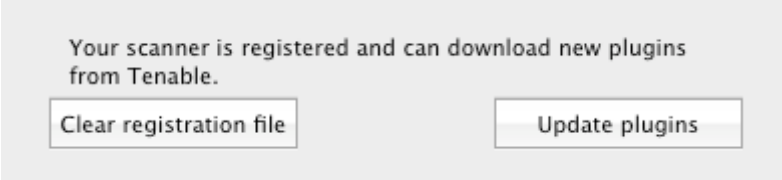
Nessus umfasst Zehntausende von Plugins (oder Skripts), die Tests auf Schwachstellen im Netzwerk und auf Hosts ausführen. Regelmäßig werden neue Sicherheitslücken gefunden, und neue Plugins werden entwickelt, um diese Sicherheitslücken zu erkennen. Damit Ihr Nessus-Scanner auf dem aktuellen Stand bleibt und stets die neuesten Plugins benutzt, müssen Sie Ihre Plugins täglich aktualisieren, denn nur so kann der Scanner zuverlässig arbeiten.

Mit der Option „**Perform a daily plugin update**" („Plugin-Update täglich ausführen") wird der Nessus-Server automatisch so konfiguriert, dass alle 24 Stunden Plugin-Updates von Tenable abgerufen werden. Dieser Vorgang erfolgt ungefähr zu der Uhrzeit, zu der Sie Nessus gestartet haben.



Sie können ein Plugin-Update auch erzwingen. Klicken Sie dazu auf die Schaltfläche „Update Plugins" („Plugins aktualisieren"):

Copyright © 2002-2011 Tenable Network Security, Inc.



Wie oft soll ich meine Plugins aktualisieren?

Im Allgemeinen ist eine tägliche Aktualisierung der Nessus-Plugins für die meisten Organisationen ausreichend. Wenn Sie jedoch stets die aktuellsten Plugins benötigen und eine fortlaufende Aktualisierung während des gesamten Tages wünschen, können Sie in einem 4-Stunden-Turnus Aktualisierungen durchführen. Eine häufigere Aktualisierung bringt praktisch keinen zusätzlichen Nutzen.

Die Aktivierung des Kontrollkästchens „Start the Nessus server when booting" („Nessus-Server beim Systemstart automatisch starten") gibt Remotebenutzern Zugriff und ermöglicht die tägliche Aktualisierung der Plugins.

NESSUS ENTFERNEN

Beenden Sie zum Entfernen von Nessus den Nessus-Dienst und löschen die folgenden Verzeichnisse:

```
/Library/Nessus
/Applications/Nessus
/Library/Receipts/Nessus*
```

Wenn Sie mit der Verwendung der UNIX-Befehlszeile auf einem Mac OS X-System nicht vertraut sind, wenden Sie sich an den Tenable-Support, um Unterstützung zu erhalten.

Es gibt Freewaretools wie „DesInstaller.app" (http://www.macupdate.com/info.php/id/7511) und „CleanApp" (http://www.macupdate.com/info.php/id/21453/cleanapp), die ebenfalls zum Entfernen von Nessus verwendet werden können. Tenable steht in keinerlei Abhängigkeitsverhältnis zu den Herstellern oder Vertreibern dieser Tools. Zudem wurden die Tools nicht speziell für die Entfernung von Nessus getestet.

NESSUS-DAEMON KONFIGURIEREN (FÜR FORTGESCHRITTENE BENUTZER)

Die Datei **`/opt/nessus/etc/nessus/nessusd.conf`** enthält verschiedene konfigurierbare Optionen. Hier legen Sie beispielsweise die maximale Anzahl von Tests und gleichzeitig zu scannenden Hosts, die von **`nessusd`** zu verwendenden Ressourcen, die Geschwindigkeit, mit der Daten gelesen werden sollen, und viele andere Optionen fest. Die Datei wird automatisch mit Standardeinstellungen erstellt. Es wird jedoch empfohlen, diese Einstellungen zu überprüfen und entsprechend der zu scannenden Umgebung anzupassen. Die vollständige Liste der Konfigurationsoptionen wird am Ende dieses Abschnitts erläutert.

Insbesondere die Parameter **`max_hosts`** und **`max_checks`** können erhebliche Auswirkungen auf die Scanfähigkeit Ihres Nessus-Systems sowie auf jene Systeme in Ihrem Netzwerk haben, die auf Sicherheitslücken gescannt werden. Gehen Sie deshalb bei der Konfiguration dieser beiden Werte mit Sorgfalt vor.

Copyright © 2002-2011 Tenable Network Security, Inc.

Nachfolgend sind die beiden Einstellungen und ihre Vorgabewerte aufgeführt, wie sie in der Datei **nessusd.conf** stehen:

```
# Maximum number of simultaneous hosts tested:
max_hosts = 40

# Maximum number of simultaneous checks against each host tested:
max_checks = 5
```

Beachten Sie, dass diese Einstellungen auf der Ebene des einzelnen Scanvorgangs außer Kraft gesetzt werden, wenn Tenable SecurityCenter oder die Nessus-Benutzeroberfläche verwendet werden. Bearbeiten Sie zur Ansicht oder Änderung dieser Optionen in einer Scanvorlage in SecurityCenter die Werte unter „Scan Template"/„Scan Options" („Scanvorlage"/„Scanoptionen"). Bearbeiten Sie auf der Nessus-Benutzeroberfläche die Scanrichtlinie und klicken Sie dann auf die Registerkarte „Options" („Optionen").

Denken Sie daran, dass die Einstellungen in **nessusd.conf** stets von den Werten in der SecurityCenter Scan Template oder den Optionen der Nessus-Webclientrichtlinie außer Kraft gesetzt werden, wenn Sie mit diesen Tools einen Scan durchführen.

Beachten Sie, dass der Parameter **max_checks** einen hartkodierten Grenzwert von 15 hat. Werte, die größer als 5 sind, führen häufig zu unerwünschten Auswirkungen, da die meisten Server eine größere Zahl aggressiver Anfragen nicht gleichzeitig bearbeiten kann.

Hinweise zu „max_hosts":

Wie der Name bereits andeutet, ist dies die maximale Anzahl von Zielsystemen, die gleichzeitig gescannt werden können. Je höher die Zahl gleichzeitig durch einen einzelnen Nessus-Scanner gescannter Systeme, desto schwerwiegender sind die Auswirkungen auf RAM, Prozessor und Netzwerkbandbreite des Scannersystems. Beachten Sie, wenn Sie den Wert für **max_hosts** festlegen, die Hardwarekonfiguration des Scannersystems und die anderen Anwendungen, die darauf ausgeführt werden.

Da auch eine Anzahl anderer Faktoren, die für Ihre Scanumgebung charakteristisch sind (z. B. die Richtlinien Ihrer Organisation in Bezug auf Scans, der sonstige Datenverkehr im Netzwerk oder die Wirkung eines bestimmten Scantyps auf Ihre gescannten Hosts), sich auf Ihre Nessus-Scans auswirken werden, werden Sie experimentieren müssen, um die optimale Einstellung für **max_hosts** zu finden.

Ein eher konservativer Ausgangspunkt für die Ermittlung der besten **max_hosts**-Einstellung in einer Unternehmensumgebung ist der Wert „20" auf einem UNIX-basierten Nessus-System und der Wert „10" auf einem Nessus-Scanner unter Windows.

Hinweise zu „max_checks":

Dieser Parameter gibt die Anzahl gleichzeitiger Tests oder Plugins an, die während des Scannens eines einzelnen Zielhosts ausgeführt werden. Beachten Sie, dass Sie durch Auswahl eines hohen Wertes die gescannten Systeme überlasten können, was jedoch auch von den beim Scan benutzten Plugins abhängig ist.

Copyright © 2002-2011 Tenable Network Security, Inc.

Multiplizieren Sie die Werte von **max_checks** und **max_hosts**, um die Anzahl gleichzeitiger Tests zu ermitteln, die zu einem beliebigen Zeitpunkt während des Scans möglicherweise ausgeführt werden. Weil **max_checks** und **max_hosts** sich gegenseitig beeinflussen, kann auch ein zu hoher Wert für **max_checks** einen Ressourcenmangel auf einem Nessus-Scannersystem verursachen. Wie bei **max_hosts** müssen Sie auch bei **max_checks** experimentieren, um die optimale Einstellung zu finden. Im Zweifelsfall sollten Sie immer einen relativ niedrigen Wert wählen.

Wenn Sie die Datei **nessusd.conf** bearbeiten, müssen Sie Nessus nachfolgend neu starten, damit die Änderungen wirksam werden.

Beim Upgrade auf Version 4.4 wird die Datei **nessusd.conf** von Nessus nicht überschrieben. Dies führt dazu, dass verschiedene Optionen nicht in die Konfigurationsdatei aufgenommen werden. Bei Optionen, die aus diesem Grund unberücksichtigt bleiben, verwendet Nessus die Standardeinstellungen, die auch Bestandteil einer Neuinstallation von Version 4.4 sind.

Die folgende Tabelle enthält kurze Erläuterungen zu allen Konfigurationsoptionen in der Datei **nessusd.conf**. Viele dieser Optionen können über die Benutzeroberfläche konfiguriert werden, wenn eine Scanrichtlinie erstellt wird. Optionen, die in Version 4.4.1 neu sind, sind fett gedruckt.

Optionen	Beschreibung
auto_update	Automatische Plugin-Updates. Falls die Option aktiviert und Nessus registriert ist, werden die aktuellen Plugins automatisch von plugins.nessus.org abgerufen. Deaktivieren Sie die Option, wenn der Scanner sich in einem isolierten Netzwerk befindet, das keine Verbindung zum Internet hat.
auto_update_delay	Wartezeit zwischen zwei Updates in Stunden. Der zulässige Mindestwert beträgt vier (4) Stunden.
purge_plugin_db	Gibt an, ob Nessus die Plugin-Datenbank bei jedem Update bereinigen soll. Wenn Sie „yes" („Ja") auswählen, dauern alle Updates wesentlich länger.
throttle_scan	Bei einer Prozessorüberlastung wird der Scanvorgang gedrosselt.
logfile	Gibt an, wo die Nessus-Logdatei gespeichert ist.
www_logfile	Gibt an, wo die Logdatei des Nessus-Webservers (Benutzeroberfläche) gespeichert ist.
log_whole_attack	Gibt an, ob jedes Detail eines Angriffs protokolliert werden soll. Dies kann zum Debuggen nützlich sein, erfordert aber sehr viel Festplattenspeicher.
dumpfile	Gibt den Speicherort einer Speicherauszugsdatei zum Debuggen der Ausgabe an (sofern generiert).
rules	Gibt an, wo die Regeldatei von Nessus gespeichert ist.

Copyright © 2002-2011 Tenable Network Security, Inc.

cgi_path	Gibt eine Liste von durch Doppelpunkte getrennten CGI-Pfaden an, die beim Testen von Webservern verwendet wird.
port_range	Gibt den zu scannenden Portbereich an. Hier können die Schlüsselwörter „default" („Standard") oder „all" („alle") sowie eine kommagetrennte Liste mit Ports oder Portbereichen angegeben werden.
optimize_test	Hierdurch wird der Testvorgang optimiert. Wenn Sie hier den Wert „no" eintragen, benötigen Scans mehr Zeit, und in der Regel werden auch mehr Fehlalarme produziert.
checks_read_timeout	Gibt den Lesetimeout für die Testsockets an.
non_simult_ports	Gibt Ports an, die nicht gleichzeitig von zwei unterschiedlichen Plugins getestet werden sollten.
plugins_timeout	Gibt die maximale Aktivitätsdauer eines Plugins (in Sekunden) an.
safe_checks	Sichere Tests nutzen die Bannererfassung, statt aktiv auf Sicherheitslücken zu testen.
auto_enable_dependencies	Hiermit werden automatisch alle Plugins aktiviert, von denen andere Plugins abhängen. Wenn diese Option deaktiviert ist, werden unter Umständen auch dann nicht alle Plugins ausgeführt, wenn sie in einer Scanrichtlinie ausgewählt wurden.
silent_dependencies	Falls diese Option aktiviert ist, geht die Liste der Plugin-Abhängigkeiten und deren Ausgaben nicht in den Bericht ein.
use_mac_addr	Legt fest, dass Hosts anhand ihrer MAC-Adresse statt der IP-Adresse identifiziert werden (dies ist praktisch in DHCP-Netzwerken).
save_knowledge_base	Speichert die Knowledge-Base zur späteren Benutzung auf der Festplatte.
plugin_upload	Gibt an, ob Administratoren Plugins hochladen können.
plugin_upload_suffixes	Suffixe von Plugins, die ein Administrator hochladen kann.
slice_network_addresses	Wenn diese Option festgelegt ist, scannt Nessus ein Netzwerk nicht inkrementell (d. h. in der Reihenfolge 10.0.0.1, 10.0.0.2, 10.0.0.3 usw.), sondern versucht, die Belastung gleichmäßig auf das Netzwerk zu verteilen. Die Reihenfolge kann dann beispielsweise 10.0.0.1, 10.0.0.127, 10.0.0.2, 10.0.0.128 usw. lauten.
listen_address	IPv4-Adresse, auf der auf eingehende Verbindungen gehorcht wird
listen_port	Port, auf dem gehorcht wird (wird vom veralteten NTP-Protokoll verwendet). Wird für Verbindungen mit NessusClients vor Version 4.2 benötigt.

Copyright © 2002-2011 Tenable Network Security, Inc.

xmlrpc_listen_port	Port, über den der Nessus Webserver horcht (wird vom neuen XMLRPC-Protokoll verwendet)
xmlrpc_idle_session_timeout	XMLRPC-Sitzungstimeout bei Leerlauf (in Minuten)
xmlrpc_min_password_len	Hiermit wird Nessus angewiesen, eine Richtlinie für die Länge eines Kennworts für Benutzer des Scanners zu erzwingen.
enable_listen_ipv4	Hiermit wird Nessus angewiesen, auf IPv4 zu horchen.
enable_listen_ipv6	Hiermit wird Nessus angewiesen, auf IPv6 zu horchen, sofern das System die IPv6-Adressierung unterstützt.
source_ip	Im Falle eines Multihomed-Systems mit unterschiedlichen IP-Adressen im selben Subnetz wird dem Nessus-Scanner mithilfe dieser Option mitgeteilt, welche Netzwerkkarte bzw. IP-Adresse er für die Tests verwenden soll. Werden mehrere IP-Adressen angegeben, dann verwendet Nessus sie nacheinander immer dann, wenn eine Verbindung hergestellt wird.
ssl_cipher_list	Hiermit wird sichergestellt, dass nur „starke" SSL-Verschlüsselungen beim Herstellen der Verbindung mit Port 1241 verwendet werden. Unterstützt werden das Schlüsselwort „strong" oder allgemeine OpenSSL-Bezeichnungen, wie sie unter http://www.openssl.org/docs/apps/ciphers.html aufgeführt sind.
disable_ntp	Deaktiviert das veraltete NTP-Protokoll.
disable_xmlrpc	Deaktiviert die neue XMLRPC-Schnittstelle (Webserverschnittstelle).
nasl_no_signature_check	Gibt an, ob Nessus alle NASL-Skripts als signiert betrachten soll. Die Auswahl „yes" ist unsicher und wird nicht empfohlen.
nasl_log_type	Leitet den Ausgabetyp der NASL-Engine in **`nessusd.dump`** um.
use_kernel_congestion_detection	Hiermit werden die Scanaktivitäten erforderlichenfalls anhand vorliegender TCP-Netzüberlastungsmeldungen zurückgefahren.
global.max_scans	Werte ungleich null geben hier die maximale Anzahl Scans an, die parallel stattfinden dürfen. **Hinweis**: Wenn diese Option nicht verwendet wird, gibt es keine Begrenzung.
global.max_web_users	Werte ungleich null geben hier die maximale Anzahl (Web-) Benutzer an, die parallel eine Verbindung herstellen dürfen. **Hinweis**: Wenn diese Option nicht verwendet wird, gibt es keine Begrenzung.
global.max_simult_tcp_sessions	Maximale Anzahl gleichzeitiger TCP-Sitzungen zwischen allen Scans. **Hinweis**: Wenn diese Option nicht verwendet wird, gibt es

Copyright © 2002-2011 Tenable Network Security, Inc.

	keine Begrenzung.
max_simult_tcp_sessions	Maximale Anzahl gleichzeitiger TCP-Sitzungen je Scan.
host.max_simult_tcp_ sessions	Maximale Anzahl gleichzeitiger TCP-Sitzungen je gescanntem Host.
reduce_connections_on_ congestion	Verringert die Anzahl der parallel ausgeführten TCP-Sitzungen, wenn im Netzwerk Überlastungen erkannt wurden.
stop_scan_on_disconnect	Beendet das Scannen eines Hosts, dessen Verbindung während des Scans getrennt wurde.
stop_scan_on_hang	Beendet einen Scan, der offenbar stehen geblieben ist.
paused_scan_timeout	Beendet einen unterbrochenen Scan zwangsweise nach der angegebenen Anzahl Minuten. Bei „0" erfolgt kein Timeout.
report_crashes	Hiermit werden anonym Berichte zu Abstürzen an Tenable übermittelt.
nessus_syn_scanner. global_throughput.max	Legt die maximale Anzahl SYN-Pakete fest, die von Nessus während eines Portscans pro Sekunde versendet werden. Wie viele Hosts dabei parallel gescannt werden, spielt keine Rolle. Geben Sie je nach Empfindlichkeit des Remotegeräts möglichst hohe Werte für die SYN-Pakete an.
qdb_mem_usage	Hiermit wird Nessus angewiesen, im Leerlauf mehr oder weniger Speicher zu verwenden. Wenn Nessus auf einem dedizierten Server ausgeführt wird, können Sie hier „high" festlegen, um mehr Speicher zuzuweisen und die Leistungsfähigkeit so zu erhöhen. Wird Nessus hingegen auf einem Computer ausgeführt, der auch noch andere Aufgaben erledigt, dann wählen Sie hier „low", um den Speicherbedarf erheblich zu beschränken. Diese Einstellung wirkt sich geringfügig auf die Leistung aus.
xmlrpc_import_feed_ policies	Wenn hier die Einstellung „no" gewählt wird, schließt Nessus die von Tenable bereitgestellten Standardscanrichtlinien nicht ein.

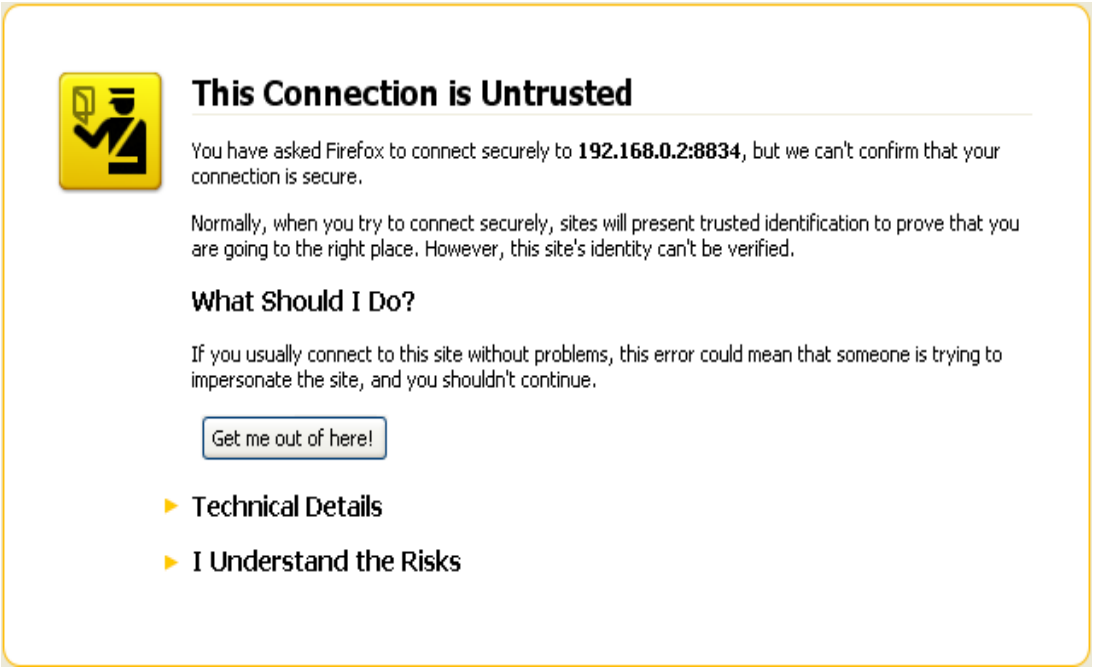
Einstellungen in der Datei **`nessusd.conf`** können durch Benutzereinstellungen in einer **`.nessusrc`**-Datei außer Kraft gesetzt werden.

Standardmäßig wird bei einem HomeFeed-Abonnement **`report_crashes`** auf „yes" gesetzt, während bei einem ProfessionalFeed-Abonnement **`report_crashes`** die Einstellung „no" festgelegt wird. Informationen, die sich auf einen Absturz in Nessus beziehen, werden an Tenable übermittelt und dort zur Beseitigung von Fehlern verwendet, um eine Software maximaler Qualität anbieten zu können. Personen- oder systembezogene Informationen werden nicht übertragen.

Copyright © 2002-2011 Tenable Network Security, Inc.

NESSUS MIT EINEM ANGEPASSTEN SSL-ZERTIFIKAT KONFIGURIEREN

Bei der Standardinstallation von Nessus wird ein selbstsigniertes SSL-Zertifikat verwendet. Wenn Sie zum ersten Mal die Weboberfläche für den Zugriff auf den Nessus-Scanner verwenden, zeigt Ihr Webbrowser eine Fehlermeldung an, laut der das Zertifikat nicht vertrauenswürdig ist:


This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.0.2:8834, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

Sie können ein angepasstes, für Ihre Organisation ausgestelltes SSL-Zertifikat verwenden, um zukünftige Warnungen im Browser zu vermeiden. Bei der Installation erstellt Nessus zwei Dateien, die das Zertifikat bilden: **`servercert.pem`** und **`serverkey.pem`**. Diese Dateien müssen durch Zertifikatsdateien ersetzt werden, die von Ihrer Organisation oder einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) generiert wurden.

Beenden Sie vor dem Ersetzen der Zertifikatsdateien den Nessus-Server. Ersetzen Sie die beiden Dateien, und starten Sie den Nessus-Server dann neu. Nachfolgend sollte bei Verbindungen mit dem Scanner keine Fehlermeldung mehr angezeigt werden, sofern das Zertifikat von einer vertrauenswürdigen CA stammt.

Die folgende Tabelle listet die Speicherorte der Zertifikatsdateien unter den einzelnen Betriebssystemen auf:

Betriebssystem	Speicherort für Zertifikatsdateien
Linux und Solaris	`/opt/nessus/com/nessus/CA/servercert.pem` `/opt/nessus/var/nessus/CA/serverkey.pem`
FreeBSD	`/usr/local/nessus/com/nessus/CA/servercert.pem` `/usr/local/nessus/var/nessus/CA/serverkey.pem`
Windows	`C:\Program Files\Tenable\Nessus\nessus\CA\`

Copyright © 2002-2011 Tenable Network Security, Inc.

Mac OS X	**/Library/Nessus/run/com/nessus/CA/servercert.pem** **/Library/Nessus/run/var/nessus/CA/serverkey.pem**

Seit Version 4.4 unterstützt Nessus SSL-Zertifikatsketten.

Sie können auch die Seite **https://[IP address]:8834/getcert** besuchen, um die Stamm-CA in Ihrem Browser zu installieren. Nachfolgend wird keine Warnung mehr angezeigt.

NESSUS OHNE INTERNETZUGANG

In diesem Abschnitt beschreiben wir die Schritte zur Registrierung des Nessus-Scanners, zur Installation des Aktivierungscodes und zum Empfang der aktuellen Plugins, falls Ihr Nessus-System keinen direkten Zugang zum Internet hat.

Aktivierungscodes, die unter Verwendung des nachfolgend beschriebenen Offlineprozesses abgerufen werden, werden an den Nessus-Scanner gebunden, der bei der Inbetriebnahme verwendet wird. Sie können das heruntergeladene Plugin-Paket nicht mit einem anderen Nessus-Scanner verwenden.

NESSUS-SCANNER REGISTRIEREN

Sie müssen Ihren Aktivierungscode für das Nessus-Abonnement entweder über Ihr Tenable Support Portal-Konto abrufen (ProfessionalFeed) oder Ihrer Registrierungs-E-Mail entnehmen (HomeFeed). Um Nessus in einer Geschäftsumgebung verwenden zu dürfen, müssen Sie den ProfessionalFeed auch dann abonnieren, wenn Sie ihn nicht direkt zu kommerziellen Zwecken einsetzen. Dies umfasst beispielsweise das Scannen Ihres Desktopcomputers bei der Arbeit oder eines Heimcomputers, der für geschäftliche Zwecke eingesetzt wird. Bitte lesen Sie den Abschnitt „Subscription Agreement" („Abonnementvertrag"), um weitere Informationen zum jeweils passenden Abonnement zu erhalten. Benutzer, die einen HomeFeed beziehen dürfen, führen die Registrierung unter http://www.nessus.org/register/ aus, indem sie dort die E-Mail-Adresse des registrierten Benutzers eingeben. Um den ProfessionalFeed zu erwerben, wenden Sie sich bitte an Tenable (E-Mail-Adresse: sales@tenable.com) oder besuchen den Onlineshop unter https://store.tenable.com/. Tenable wird Ihnen dann einen Aktivierungscode für den ProfessionalFeed zukommen lassen.

Beachten Sie, dass Sie nur einen Aktivierungscode je Scanner einsetzen können, sofern die Scanner nicht über SecurityCenter verwaltet werden.

Sobald Sie über den Aktivierungscode verfügen, führen Sie den folgenden Befehl auf dem System aus, auf dem Nessus läuft:

Windows:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --challenge
```

Linux und Solaris:

```
# /opt/nessus/bin/nessus-fetch --challenge
```

Copyright © 2002-2011 Tenable Network Security, Inc.

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --challenge
```

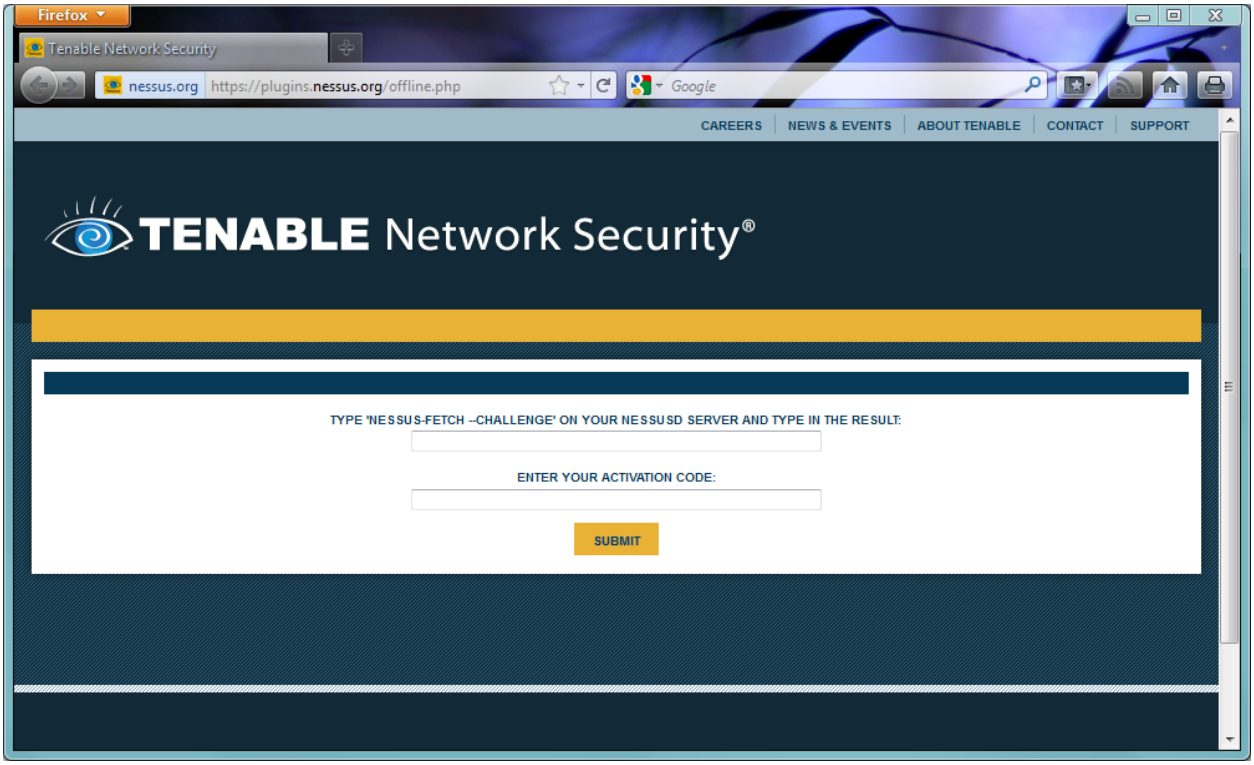
Mac OS X:

```
# /Library/Nessus/run/bin/nessus-fetch --challenge
```

Hiermit wird eine Zeichenfolge erstellt, die als „Challenge" bezeichnet wird und wie folgt aussieht:

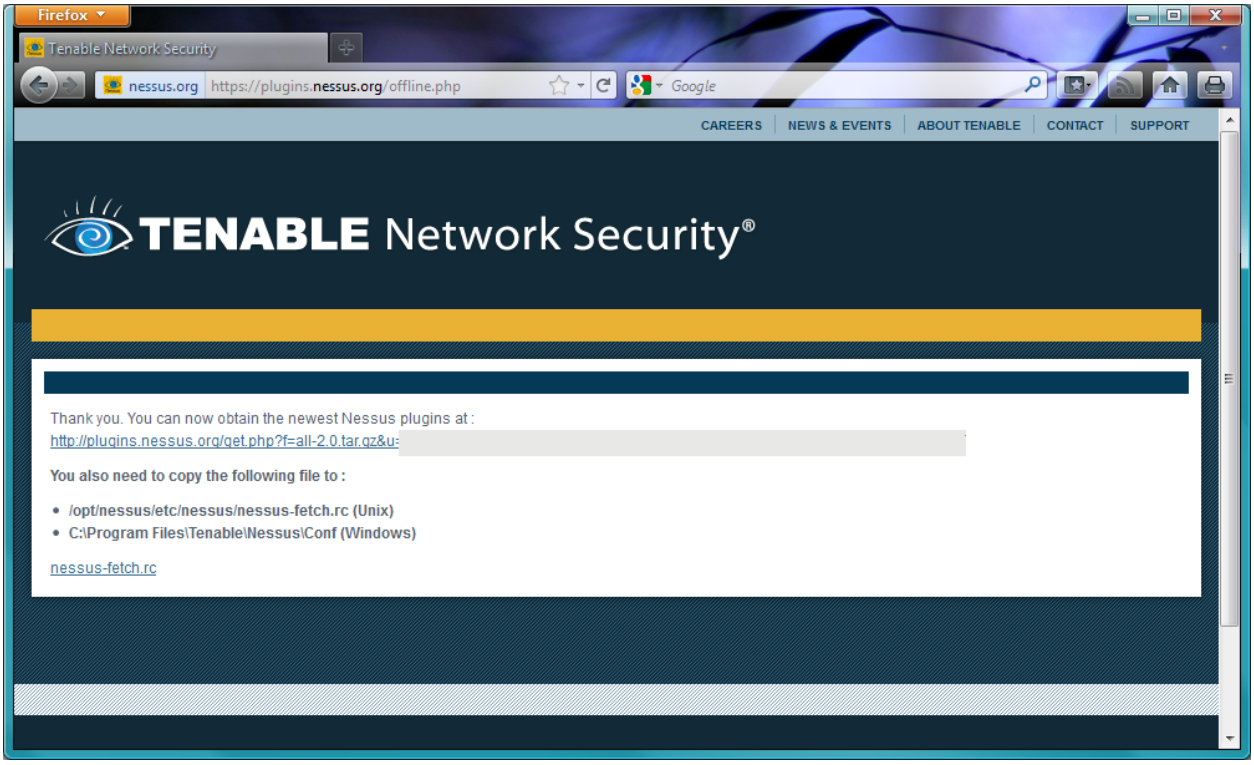
```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Rufen Sie dann die Seite https://plugins.nessus.org/offline.php auf und kopieren die Challenge sowie den zuvor erhaltenen Aktivierungscode über die Zwischenablage in die entsprechenden Textfelder:



Copyright © 2002-2011 Tenable Network Security, Inc.

Daraufhin wird eine URL ähnlich der in der folgenden Bildschirmabbildung gezeigten generiert:



Auf diesem Bildschirm haben Sie die Möglichkeit, die aktuellen Nessus-Plugins als gepackte Datei (**`all-2.0.tar.gz`**) herunterzuladen. Außerdem finden Sie am unteren Bildschirmrand einen Link zur Datei **`nessus-fetch.rc`**.

Diese URL müssen Sie speichern, denn Sie benötigen sie immer dann, wenn Sie – wie im nächsten Abschnitt beschrieben – Ihre Plugins aktualisieren möchten.

Ein Registrierungscode, der für Offlineupdates verwendet wird, kann im Nessus Server Manager nicht für denselben Nessus-Scannerserver verwendet werden.

Wenn Sie den Registrierungscode für den jeweiligen Scanner überprüfen müssen, können Sie jederzeit die Option **`--code-in-use`** für das Programm **`nessus-fetch`** verwenden.

Kopieren Sie die Datei **`nessus-fetch.rc`** auf den Host, auf dem Nessus ausgeführt wird, in das folgende Verzeichnis:

Windows:

`C:\Program Files\Tenable\Nessus\conf`

Linux und Solaris:

`/opt/nessus/etc/nessus/`

Copyright © 2002-2011 Tenable Network Security, Inc.

FreeBSD:

/usr/local/nessus/etc/nessus/

Mac OS X:

/Library/Nessus/run/etc/nessus/

Die Datei **nessus-fetch.rc** muss nur einmal kopiert werden. Zukünftige Downloads von Nessus-Plugins hingegen müssen jeweils in das entsprechende Verzeichnis kopiert werden (siehe Beschreibung im nächsten Abschnitt).

Beachten Sie, dass Nessus nach der Registrierung standardmäßig alle 24 Stunden versuchen wird, die Plugins zu aktualisieren. Wenn Sie diesen Versuch, online zu gehen, unterbinden möchten, bearbeiten Sie einfach die Datei **nessusd.conf**. Sie müssen dort die Option „**auto_update**" auf „„**no**" setzen.

AKTUELLE PLUGINS BEZIEHEN UND INSTALLIEREN

Führen Sie diesen Schritt jedes Mal aus, wenn Sie ein Offlineupdate Ihrer Plugins ausführen.

Windows

Zum Abrufen der neuesten Plugins rufen Sie die URL auf, die im vorherigen Schritt angegeben wurde, laden die Datei „**all-2.0.tar.gz**" herunter und speichern sie im Verzeichnis **C:\Program Files\Tenable\Nessus**. Geben Sie nun zum Installieren der Plugins folgenden Befehl ein:

```
C:\Program Files\Tenable\Nessus>nessus-update-plugins.exe all-2.0.tar.gz
Expanding all-2.0.tar.gz
Done. You need to restart the Nessus server for the changes to take effect

C:\Program Files\Tenable\Nessus>
```

Danach beenden Sie mithilfe von Nessus Server Manager den Nessus-Server und starten ihn neu.

Nach der Installation der Plugins können Sie die Datei **all-2.0.tar.gz** eigentlich löschen; Tenable empfiehlt jedoch, die jeweils aktuellste Version der heruntergeladenen Plugin-Datei für den Fall beizubehalten, dass sie noch einmal benötigt wird.

Nun stehen Ihnen die aktuellen Plugins zur Verfügung. Jedes Mal, wenn Sie ein Update Ihrer Plugins ausführen möchten, müssen Sie die angegebene URL aufrufen, die TAR-Datei mit den Plugins herunterladen, sie auf das System kopieren, auf dem Nessus ausgeführt wird, und den obigen Befehl eingeben.

Linux, Solaris und FreeBSD

Rufen Sie zum Erhalt der neuesten Plugins die URL auf, die im vorherigen Schritt angegeben wurde, laden die Datei „**"all-2.0.tar.gz**" herunter und speichern sie im Verzeichnis **/opt/nessus/sbin/** (bzw. in **/usr/local/nessus/sbin/** für FreeBSD). Geben Sie nun zum Installieren der Plugins folgenden Befehl ein:

Copyright © 2002-2011 Tenable Network Security, Inc.

Linux und Solaris:

```
# /opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
```

Starten Sie dann den Nessus-Prozess über die Befehlszeile neu, damit Nessus ab sofort die neuen Plugins verwendet. Hinweise zum Neustart des Nessus-Daemons finden Sie in den Abschnitten „Den Nessus-Daemon beenden" und „Den Nessus-Daemon starten".

Nach der Installation der Plugins können Sie die Datei **all-2.0.tar.gz** eigentlich löschen; Tenable empfiehlt jedoch, die jeweils aktuellste Version der heruntergeladenen Plugin-Datei für den Fall beizubehalten, dass sie noch einmal benötigt wird.

Nun stehen Ihnen die aktuellen Plugins zur Verfügung. Jedes Mal, wenn Sie ein Update Ihrer Plugins ausführen möchten, müssen Sie die angegebene URL aufrufen, das TAR-Archiv herunterladen, es auf das System kopieren, auf dem Nessus ausgeführt wird, und den obigen Befehl eingeben.

Mac OS X

Rufen Sie zum Erhalt der neuesten Plugins die URL auf, die im vorherigen Schritt angegeben wurde, laden die Datei „**all-2.0.tar.gz**" herunter und speichern sie im Verzeichnis **/Library/Nessus/run/sbin/**. Geben Sie nun zum Installieren der Plugins folgenden Befehl ein:

```
# /Library/Nessus/run/sbin/nessus-update-plugins all-2.0.tar.gz
```

Danach beenden Sie mithilfe von Nessus Server Manager den Nessus-Server und starten ihn neu.

Nach der Installation der Plugins können Sie die Datei **all-2.0.tar.gz** eigentlich löschen; Tenable empfiehlt jedoch, die jeweils aktuellste Version der heruntergeladenen Plugin-Datei für den Fall beizubehalten, dass sie noch einmal benötigt wird.

Nun stehen Ihnen die aktuellen Plugins zur Verfügung. Jedes Mal, wenn Sie ein Update Ihrer Plugins ausführen möchten, müssen Sie die angegebene URL aufrufen, das TAR-Archiv mit den Plugins herunterladen, es auf das System kopieren, auf dem Nessus ausgeführt wird, und den obigen Befehl eingeben.

MIT SECURITYCENTER ARBEITEN

SECURITYCENTER IM ÜBERBLICK

Tenable SecurityCenter ist eine webbasierte Verwaltungskonsole, die den Prozess der Sicherheitslückenerkennung und -verwaltung, Ereignis- und Logdateiverwaltung, Compliance-Überwachung und eine Berichtserstellungsfunktion für alle genannten Vorgänge auf einer einheitlichen Oberfläche zusammenfasst. SecurityCenter ermöglicht eine effiziente Kommunikation sicherheitsrelevanter Ereignisse an IT-, Verwaltungs- und Auditteams.

SecurityCenter unterstützt die koordinierte Nutzung mehrerer Nessus-Scanner, um Netzwerke praktisch beliebiger Größe regelmäßig zu scannen. Mithilfe der Nessus-API (einer

Copyright © 2002-2011 Tenable Network Security, Inc.

angepassten Implementierung des XML-RPC-Protokolls) kommuniziert SecurityCenter mit den zugeordneten Nessus-Scannern, um Anweisungen an diese zu übermitteln und Resultate abzurufen.

SecurityCenter ermöglicht mehreren Benutzern und Administratoren unterschiedlicher Sicherheitsstufen die Freigabe von Informationen zu Sicherheitslücken, eine Priorisierung der Sicherheitslücken, das Auflisten von Netzwerk-Assets, die kritische Sicherheitsprobleme aufweisen, das Empfehlen von durch Systemadministratoren zur Behebung dieser Sicherheitsprobleme durchzuführenden Maßnahmen und schließlich die Überprüfung, ob die Sicherheitslücke geschlossen wurde. SecurityCenter ruft außerdem über die Log Correlation Engine Daten von zahlreichen führenden Intrusion-Detection-Systemen wie Snort oder ISS ab.

Außerdem kann SecurityCenter auch passive Sicherheitslückeninformationen vom Tenable Passive Vulnerability Scanner abrufen, damit Endbenutzer neue Hosts, Anwendungen, Sicherheitslücken und unbefugtes Eindringen auch ohne aktives Scannen mit Nessus ermitteln können.

NESSUS FÜR DIE KOOPERATION MIT SECURITYCENTER KONFIGURIEREN

Damit ein Nessus-Scanner durch SecurityCenter gesteuert werden kann, müssen für das Hochladen von Plugins und die Durchführung eines Scans ein Benutzername und das zugehörige Kennwort angegeben werden. Der betreffende Benutzer muss mithilfe des Prozesses „**nessus-adduser**“ als Administrator konfiguriert worden sein, damit sichergestellt ist, dass er über die Berechtigungen für das Hochladen von Plugins und für andere administrative Funktionen verfügt.

Auch wenn ein Nessus-Scanner lediglich für die Überprüfung bestimmter IP-Bereiche konfiguriert ist, kann er trotzdem von SecurityCenter verwendet werden. Wenn in Security Center allerdings der Versuch gestartet wird, Scans außerhalb dieser Bereiche auszuführen, werden keine Daten zu Sicherheitslücken gemeldet.

UNIX/Mac OS X

Befolgen Sie in Systemen mit der UNIX-Befehlszeile die Anweisungen zum Hinzufügen von Benutzern im Abschnitt „Einen Nessus-Benutzer erstellen“. Vergewissern Sie sich, dass der erstellte Benutzer ein Administrator ist.

Befolgen Sie in Mac OS X-Systemen die Anweisungen zum Erstellen eines Benutzers im Abschnitt „Nessus-Benutzer erstellen und verwalten“. Nessus-Benutzer werden auf einem Mac standardmäßig mit Administratorrechten erstellt.

Windows

Nessus für das Horchen als Netzwerk-Daemon konfigurieren

Nessus kann für eine Kommunikation mit SecurityCenter konfiguriert werden. Zu diesem Zweck müssen Sie zwei Schritte durchführen. Zunächst müssen Sie ein Konto für die Anmeldung von SecurityCenter bei Nessus erstellen, und dann müssen Sie den Nessus-Dienst so konfigurieren, dass er auf eingehende Netzwerkverbindungen von SecurityCenter horcht.

Benutzerkonten unter Windows hinzufügen

Wenn Sie Nessus für Windows in Verbindung mit SecurityCenter einsetzen, müssen Sie einen Benutzer über die Befehlszeile erstellen und ihn registrieren. Auf diese Weise kann der Administrator den **nessusd**-Dienst und SecurityCenter starten, um die Plugins hochzuladen.

Copyright © 2002-2011 Tenable Network Security, Inc.

Öffnen Sie dazu eine DOS-Eingabeaufforderung (Start > Ausführen > „cmd" eingeben) und wechseln in das Verzeichnis **C:\Program Files\Tenable\Nessus**. Geben Sie die folgenden Befehle ein, um einen Benutzer hinzuzufügen und Nessus anzuweisen, Plugins bei SecurityCenter abzurufen:

```
C:\Program Files\Tenable\Nessus>nessus-adduser.exe
Login : admin
Authentication (pass/cert) : [pass]
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins,
       etc...)
 (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that admin has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)


Login             : admin
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
User added
#
```

SecurityCenter-Benutzer müssen stets Administratoren sein.

Den Nessus-Dienst unter Windows aktivieren

Nach dem Hinzufügen des Nessus-Benutzers muss der Nessus-Server so konfiguriert werden, dass der Nessus-Dienst aktiviert wird. Erst danach kann SecurityCenter den Nessus-Server tatsächlich hinzufügen. Geben Sie den folgenden Befehl ein:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --security-center
nessusd can now be started, SecurityCenter will upload the plugins

C:\Program Files\Tenable\Nessus>
```

Starten Sie mithilfe des Windows-Dienst-Managers den Dienst „Tenable Nessus". Wenn Sie überprüfen möchten, dass Nessus auf Port 1241 horcht, verwenden Sie den Befehl **„netstat -an | findstr 1241"** wie nachfolgend gezeigt auf der Windows-Befehlszeile:

```
C:\Documents and Settings\admin>netstat -an | findstr 1241
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
```

Copyright © 2002-2011 Tenable Network Security, Inc.

Achten Sie darauf, dass die Ausgabe „0.0.0.0:1241" enthält; dies ist ein Hinweis darauf, dass ein Server auf diesem Port horcht. Der Nessus-Server kann SecurityCenter nun über die SecurityCenter-Weboberfläche hinzugefügt werden.

Hostbasierte Firewalls

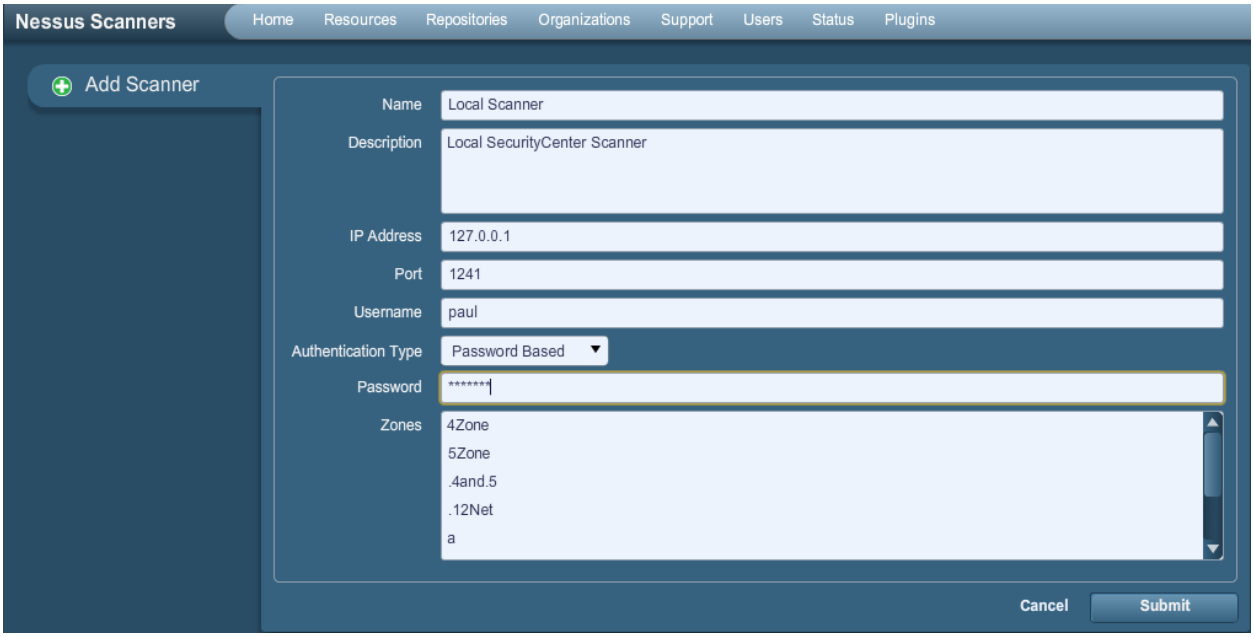
Wenn Ihr Nessus-Server mit einer lokalen Firewall wie beispielsweise Zone Alarm, Sygate, BlackICE, der Windows XP-Firewall oder einer anderen Firewallsoftware konfiguriert ist, müssen Verbindungsanfragen von der IP-Adresse von SecurityCenter zugelassen werden.

Standardmäßig wird Port 1241 verwendet. Auf Systemen unter Microsoft XP Service Pack 2 und höher erhält der Benutzer nach einem Klick auf das „**Sicherheitscenter**" in der „**Systemsteuerung**" die Möglichkeit, die Einstellungen der Windows-Firewall zu verwalten. Um Port 1241 zu öffnen, wählen Sie die Registerkarte „**Ausnahmen**" aus und fügen Sie der Liste Port 1241 hinzu.

SECURITYCENTER FÜR DIE KOOPERATION MIT NESSUS KONFIGURIEREN

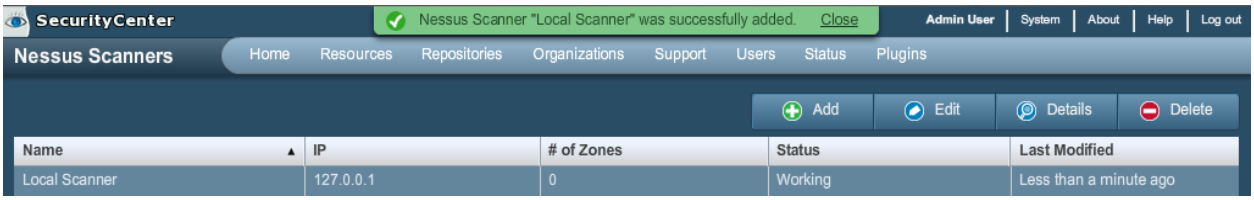
Ein Nessus-Server kann über die SecurityCenter-Verwaltungsoberfläche hinzugefügt werden. Mithilfe dieser Oberfläche lässt sich SecurityCenter so konfigurieren, dass von hier aus auf praktisch jeden Nessus-Scanner zugegriffen und dieser gesteuert werden kann. Klicken Sie auf die Registerkarte „Resources" („Ressourcen") und dann auf „**Nessus Scanners**". Klicken Sie auf „**Add**" („Hinzufügen"), um das Dialogfeld „Add Scanner" („Scanner hinzufügen") zu öffnen. Angegeben werden müssen die IP-Adresse des Nessus-Scanners, der Nessus-Port (Standard: 1241), der Anmeldename des Administrators, der Authentifizierungstyp und das (bei der Konfiguration von Nessus erstellte) Kennwort. Die Kennwortfelder sind nicht verfügbar, wenn die Authentifizierung via SSL-Zertifikat (Option „SSL Certificate") ausgewählt wird. Außerdem können unter „Zones" Zonen festgelegt werden, denen der Nessus-Scanner zugeordnet werden kann.

Nachfolgend gezeigt ist eine Bildschirmabbildung der SecurityCenter-Seite zum Hinzufügen von Scannern:



Nach dem erfolgreichen Hinzufügen des Scanners wird die folgende Seite angezeigt:

Copyright © 2002-2011 Tenable Network Security, Inc.


SecurityCenter
Nessus Scanner "Local Scanner" was successfully added. Close
Admin User | System | About | Help | Log out
Nessus Scanners
Home Resources Repositories Organizations Support Users Status Plugins
Add Edit Details Delete
Name IP # of Zones Status Last Modified
Local Scanner 127.0.0.1 0 Working Less than a minute ago

Weitere Informationen finden Sie im „SecurityCenter-Administrationshandbuch".

PROBLEMBEHANDLUNG BEI NESSUS FÜR WINDOWS

INSTALLATIONS- UND UPGRADEPROBLEME

Problem: Laut der Logdatei „nessusd.messages" wurde „nessusd" gestartet, was offensichtlich aber nicht zutrifft.

Lösung: Die Meldung „nessusd <Version> started" („nessusd <Version> wurde gestartet") gibt nur an, dass das Programm **`nessusd`** ausgeführt wurde. Die Meldung „nessusd is ready" hingegen besagt, dass der Nessus-Server ausgeführt wird und Verbindungen annehmen kann.

Problem: Ich erhalte bei dem Versuch, Nessus Windows zu installieren, folgende Fehlermeldung:

„1607: Unable to install InstallShield Scripting Runtime" („Die InstallShield Scripting-Laufzeit kann nicht installiert werden")

Lösung: Dieser Fehlercode wird erzeugt, wenn der WMI-Dienst (Windows Management Instrumentation) deaktiviert wurde. Vergewissern Sie sich, dass der Dienst ausgeführt wird.

Wenn der WMI-Dienst ausgeführt wird, kommt als Ursache ein Konflikt zwischen den Einstellungen des Microsoft Windows-Betriebssystems und dem InstallShield-Produkt in Frage, mit dem Nessus Windows installiert und entfernt wird. Knowledge-Base-Artikel, die mögliche Ursachen und Lösungen zu diesem Problem beschreiben, wurden sowohl von Microsoft als auch von InstallShield veröffentlicht.

- Microsoft Knowledge-Base-Artikel 910816:
  http://support.microsoft.com/?scid=kb;en-us;910816

- InstallShield Knowledge-Base-Artikel Q108340:
  http://consumer.installshield.com/kb.asp?id=Q108340

PROBLEME BEIM SCANNEN

Problem: Ich kann über meine PPP- oder PPTP-Verbindung keine Scans ausführen.

Lösung: Gegenwärtig wird diese Vorgehensweise nicht unterstützt. Zukünftige Versionen von Nessus Windows werden jedoch eine solche Funktionalität enthalten.

Copyright © 2002-2011 Tenable Network Security, Inc.

Problem: Ein Virenscan meines Systems meldet eine große Zahl Viren in Nessus Windows.

Lösung: Bestimmte Antivirenprogramme melden einige Nessus-Plugins als Viren. Schließen Sie das Plugin-Verzeichnis vom Virenscan aus. Das Verzeichnis enthält keine ausführbaren Dateien.

Problem: Ich scanne ein ungewöhnliches Gerät (z. B. einen RAID-Controller), und der Scan wird abgebrochen, weil es von Nessus als Drucker erkannt wird.

Lösung: Deaktivieren Sie die Option „Safe Checks" in der Scanrichtlinie, bevor Sie das Gerät scannen. Der Scan eines Druckers führt gewöhnlich dazu, dass der Drucker neu gestartet werden muss. Aus diesem Grund werden, wenn „Safe Checks" festgelegt ist, als Drucker erkannte Geräte nicht gescannt.

Problem: Bei SYN-Scans wird offenbar nicht darauf gewartet, dass die Portverbindung in Nessus Windows hergestellt wird.

Lösung: Dies ist insofern korrekt, als bei einem SYN-Scan keine vollständige TCP-Verbindung aufgebaut wird. Allerdings hat dies keine Auswirkungen auf die Scanergebnisse.

Problem: Welche Faktoren wirken sich bei der Durchführung eines Scans auf die Leistung aus, wenn Nessus Windows auf einem Windows XP-System ausgeführt wird?

Lösung: Microsoft hat an Windows XP SP2 und 3 (und zwar sowohl bei der Home- als auch bei der Professional-Version) Änderungen vorgenommen, die die Leistungsfähigkeit von Nessus Windows beeinträchtigen und Fehlalarme auslösen können. Der TCP/IP-Stapel beschränkt nun die Anzahl gleichzeitiger unvollständiger ausgehender TCP-Verbindungsversuche. Wenn dieses Limit erreicht wurde, werden nachfolgende Verbindungsversuche in eine Warteschlange eingereiht und mit festgelegter Geschwindigkeit (zehn Verbindungsversuche pro Sekunde) aufgelöst. Wenn die Warteschlange zu lang wird, werden möglicherweise Verbindungsanfragen verworfen. Die folgende Microsoft TechNet-Seite enthält weitere Informationen:

http://technet.microsoft.com/en-us/library/bb457156.aspx

Dies hat zur Folge, dass ein Nessus-Scan unter Windows XP unter Umständen Fehlalarme produziert, denn Windows XP gestattet lediglich zehn neue Verbindungen pro Sekunde, die nicht abgeschlossen sind (d. h. den SYN-Zustand aufweisen). Zur Genauigkeitsverbesserung wird empfohlen, die Drosselungseinstellungen für Portscans bei Nessus auf einem Windows XP-System auf die folgenden Werte zu verringern (Sie finden die Parameter in der Scankonfiguration der jeweiligen Scanrichtlinie):

Max number of hosts (maximale Anzahl Hosts): 10
Max number of security checks (maximale Anzahl Sicherheitstests): 4

Um die Leistungsfähigkeit und die Zuverlässigkeit von Scans zu steigern, wird dringend empfohlen, Nessus Windows auf einem Serverprodukt der Microsoft Windows-Familie (z. B. Windows Server 2003 oder Windows Server 2008) zu installieren.

Copyright © 2002-2011 Tenable Network Security, Inc.

WEITERE INFORMATIONEN

Tenable hat eine Reihe von Dokumenten erstellt, in denen die Bereitstellung, die Konfiguration, der Betrieb und die Testmethoden von Nessus ausführlich beschrieben werden. Es sind diese:

- **Nessus-Benutzerhandbuch** (beschreibt Konfiguration und Bedienung der Nessus-Benutzeroberfläche)
- **Authentifizierte Nessus-Tests für UNIX und Windows** (enthält Informationen zur Durchführung authentifizierter Netzwerkscans mit dem Nessus-Sicherheitslückenscanner)
- **Nessus-Compliancetests** (allgemeiner Leitfaden zum Verständnis und zur Durchführung von Compliancetests mithilfe von Nessus und SecurityCenter)
- **Nessus-Referenzhandbuch für Compliancetests** (umfassender Leitfaden zur Syntax von Nessus-Compliancetests)
- **Nessus V2-Dateiformat** (beschreibt die Struktur des `.nessus`-Dateiformats, das mit Nessus 3.2 und NessusClient 3.2 eingeführt wurde)
- **Nessus XML-RPC-Protokollspezifikation** (beschreibt das XML-RPC-Protokoll und die Schnittstelle in Nessus)
- **Compliance-Überwachung in Echtzeit** (erläutert, wie die Lösungen von Tenable Sie bei der Erfüllung zahlreicher gesetzlicher Vorschriften und Finanzstandards unterstützt)

Setzen Sie sich mit uns in Verbindung – via E-Mail (support@tenable.com, sales@tenable.com) oder über unsere Website unter http://www.tenable.com/.

Copyright © 2002-2011 Tenable Network Security, Inc.

LIZENZERKLÄRUNGEN DRITTER

Nachfolgend finden Sie Informationen zu Softwarepaketen von Drittanbietern, die Tenable zur Verwendung mit Nessus bereitstellt. Drittanbieterkomponenten, die von Tenable nicht als urheberrechtlich geschützt gekennzeichnet sind, unterliegen anderen Lizenzbestimmungen, die in der Dokumentation angegeben sind.

Drittanbieter-Plugins werden als „Plugins zur Erkennung von Sicherheitslücken" betrachtet und sind nachfolgend aufgeführt.

Abschnitt 1 (a) der Nessus-Lizenzvereinbarung lautet:

Alle Plugins und Komponenten, die von Tenable nicht als urheberrechtlich geschützt gekennzeichnet sind, sind keine Plugins im Sinne der Definition dieser Bezugsvereinbarung und unterliegen anderen Lizenzbestimmungen.

Abschnitt 1 (b) (i) der Nessus-Lizenzvereinbarung lautet:

Das Abonnement schließt Programme zur Erkennung von Sicherheitslücken ein, die nicht von Tenable oder seinen Lizenzgebern entwickelt wurden und die im Rahmen separater Vereinbarungen für Sie lizenziert werden. Die Gültigkeit der Bestimmungen der vorliegenden Bezugsvereinbarung erstreckt sich nicht auf solche Programme zur Erkennung von Sicherheitslücken.

Teile der vorliegenden Netzwerksicherheitssoftware von Tenable verwenden unter Umständen das folgende urheberrechtlich geschützte Material, dessen Verwendung hiermit anerkannt wird:

In Teilen: Copyright (c) 1997-2008 University of Cambridge (libpcre)

Die Weitergabe und Verwendung in Quellcode- und Binärform sind mit oder ohne Änderungen zulässig, sofern die folgenden Bedingungen erfüllt sind:

- Die Weitergabe des Quellcodes muss den obigen Copyrighthinweis, diese Bedingungsliste und den folgenden Haftungsausschluss enthalten.
- Bei Weitergabe in binärer Form müssen der obige Copyrighthinweis, diese Bedingungsliste und der folgende Haftungsausschluss in der Dokumentation und/oder anderen Materialien, die Bestandteil der Distribution sind, wiedergegeben werden.
- Weder der Name der University of Cambridge noch der Name „Google, Inc." noch die Namen von Mitarbeitern dürfen ohne vorherige schriftliche Genehmigung zur Bewerbung von Produkten verwendet werden, die aus dieser Software abgeleitet wurden.

DIESE SOFTWARE WIRD VON DEN COPYRIGHTINHABERN UND MITARBEITERN WIE BESEHEN („AS IS") BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUSGESCHLOSSEN. IN KEINEM FALL ÜBERNEHMEN DER COPYRIGHTINHABER ODER DIE MITARBEITER DIE VERTRAGLICHE, DELIKTSRECHTLICHE, VERSCHULDENSUNABHÄNGIGE ODER ANDERWEITIGE HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE ODER BESONDERE SCHÄDEN, STRAFSCHADENSERSATZ BEGRÜNDENDE SCHÄDEN SOWIE FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE ERSATZBESCHAFFUNG VON GÜTERN ODER DIENSTLEISTUNGEN, DEN VERLUST DES GEBRAUCHSWERTS ODER VON DATEN,

Copyright © 2002-2011 Tenable Network Security, Inc.

ENTGANGENEN GEWINN ODER BETRIEBSUNTERBRECHUNG), DIE IM ZUSAMMENHANG MIT DER BENUTZUNG DIESER SOFTWARE ENTSTEHEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE, UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WURDEN.

In Teilen: Copyright (c) 2000 The NetBSD Foundation, Inc. Alle Rechte vorbehalten.

DIESE SOFTWARE WIRD VON DER NETBSD FOUNDATION, INC. UND MITARBEITERN WIE BESEHEN („AS IS") BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUSGESCHLOSSEN. IN KEINEM FALL ÜBERNEHMEN DIE FOUNDATION ODER DIE MITARBEITER DIE VERTRAGLICHE, DELIKTRECHTLICHE, VERSCHULDENSUNABHÄNGIGE ODER ANDERWEITIGE HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE ODER BESONDERE SCHÄDEN, STRAFSCHADENSERSATZ BEGRÜNDENDE SCHÄDEN SOWIE FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE ERSATZBESCHAFFUNG VON GÜTERN ODER DIENSTLEISTUNGEN, DEN VERLUST DES GEBRAUCHSWERTS ODER VON DATEN, ENTGANGENEN GEWINN ODER BETRIEBSUNTERBRECHUNG), DIE IM ZUSAMMENHANG MIT DER BENUTZUNG DIESER SOFTWARE ENTSTEHEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE, UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WURDEN.

In Teilen: Copyright (c) 1995-1999 Kungliga Tekniska Hogskolan (Königliches Institut für Technologie, Stockholm, Schweden). Alle Rechte vorbehalten.

DIESE SOFTWARE WIRD VOM INSTITUT UND SEINEN MITARBEITERN WIE BESEHEN („AS IS") BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUSGESCHLOSSEN. IN KEINEM FALL ÜBERNEHMEN DAS INSTITUT ODER DESSEN MITARBEITER DIE VERTRAGLICHE, DELIKTRECHTLICHE, VERSCHULDENSUNABHÄNGIGE ODER ANDERWEITIGE HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE ODER BESONDERE SCHÄDEN, STRAFSCHADENSERSATZ BEGRÜNDENDE SCHÄDEN SOWIE FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE ERSATZBESCHAFFUNG VON GÜTERN ODER DIENSTLEISTUNGEN, DEN VERLUST DES GEBRAUCHSWERTS ODER VON DATEN, ENTGANGENEN GEWINN ODER BETRIEBSUNTERBRECHUNG), DIE IM ZUSAMMENHANG MIT DER BENUTZUNG DIESER SOFTWARE ENTSTEHEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE, UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WURDEN.

In Teilen: Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. und Clark Cooper
In Teilen: Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat-Maintainers.

DIESE SOFTWARE WIRD WIE BESEHEN („AS IS") BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER SIND AUSGESCHLOSSEN. IN KEINEM FALL SIND DIE AUTOREN ODER COPYRIGHTINHABER VERTRAGLICH, DELIKTRECHTLICH ODER ANDERWEITIG FÜR FORDERUNGEN, SCHÄDEN ODER SONSTIGE ANSPRÜCHE HAFTBAR, DIE IM

Copyright © 2002-2011 Tenable Network Security, Inc.

ZUSAMMENHANG MIT DER SOFTWARE, AUS DEREN GEBRAUCH ODER ANDERWEITIGER VERWENDUNG DER SOFTWARE ENTSTEHEN.

Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit entwickelt wurde. (http://www.openssl.org/) Copyright (c) 1998-2007 The OpenSSL Project. Alle Rechte vorbehalten.

DIESE SOFTWARE WIRD DURCH DAS OpenSSL PROJECT WIE BESEHEN („AS IS") BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUSGESCHLOSSEN. IN KEINEM FALL ÜBERNEHMEN DAS OpenSSL PROJECT ODER SEINE MITARBEITER DIE VERTRAGLICHE, DELIKTRECHTLICHE, VERSCHULDENSUNABHÄNGIGE ODER ANDERWEITIGE HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE ODER BESONDERE SCHÄDEN, STRAFSCHADENSERSATZ BEGRÜNDENDE SCHÄDEN SOWIE FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE ERSATZBESCHAFFUNG VON GÜTERN ODER DIENSTLEISTUNGEN, DEN VERLUST DES GEBRAUCHSWERTS ODER VON DATEN, ENTGANGENEN GEWINN ODER BETRIEBSUNTERBRECHUNG), DIE IM ZUSAMMENHANG MIT DER BENUTZUNG DIESER SOFTWARE ENTSTEHEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE, UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WURDEN.

In Teilen: Copyright (c) 1998-2003 Daniel Veillard. Alle Rechte vorbehalten.

Hiermit wird jeder Person, die eine Kopie der Software und der zugehörigen Dokumentationsdateien (im Folgenden: „Software") erhält, unentgeltlich das Recht eingeräumt, mit der Software zu handeln, einschließlich, aber nicht beschränkt auf das Nutzen, Kopieren, Ändern, Fusionieren, Veröffentlichen, Vertreiben, Vergeben von Unterlizenzen und/oder Verkaufen von Kopien der Software und die gleichen Rechte Personen einzuräumen, die diese Software erhalten, sofern die folgenden Bedingungen erfüllt sind:

Der obige Copyrightvermerk und dieser Erlaubnisvermerk sind in alle Kopien oder Teilkopien der Software einzuschließen.

DIESE SOFTWARE WIRD WIE BESEHEN („AS IS") BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER SIND AUSGESCHLOSSEN. IN KEINEM FALL IST DANIEL VEILLARD VERTRAGLICH, DELIKTRECHTLICH ODER ANDERWEITIG FÜR FORDERUNGEN, SCHÄDEN ODER SONSTIGE ANSPRÜCHE HAFTBAR, DIE IM ZUSAMMENHANG MIT DER SOFTWARE, AUS DEREN GEBRAUCH ODER ANDERWEITIGER VERWENDUNG DER SOFTWARE ENTSTEHEN.

In Teilen: Copyright (c) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard. Alle Rechte vorbehalten.

Hiermit wird jeder Person, die eine Kopie der Software und der zugehörigen Dokumentationsdateien (im Folgenden: „Software") erhält, unentgeltlich das Recht eingeräumt, mit der Software zu handeln, einschließlich, aber nicht beschränkt auf das Nutzen, Kopieren, Ändern, Fusionieren, Veröffentlichen, Vertreiben, Vergeben von Unterlizenzen und/oder

Verkaufen von Kopien der Software und die gleichen Rechte Personen einzuräumen, die diese Software erhalten, sofern die folgenden Bedingungen erfüllt sind:

Der obige Copyrightvermerk und dieser Erlaubnisvermerk sind in alle Kopien oder Teilkopien der Software einzuschließen.

DIESE SOFTWARE WIRD WIE BESEHEN („AS IS“) BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER SIND AUSGESCHLOSSEN. IN KEINEM FALL SIND DIE AUTOREN VERTRAGLICH, DELIKTRECHTLICH ODER ANDERWEITIG FÜR FORDERUNGEN, SCHÄDEN ODER SONSTIGE ANSPRÜCHE HAFTBAR, DIE IM ZUSAMMENHANG MIT DER SOFTWARE, AUS DEREN GEBRAUCH ODER ANDERWEITIGER VERWENDUNG DER SOFTWARE ENTSTEHEN.

Copyright © 2002-2011 Tenable Network Security, Inc.

WISSENSWERTES ZU TENABLE NETWORK SECURITY

Tenable Network Security gehört zu den Marktführern im Bereich Unified Security Monitoring. Das Unternehmen entwickelt den Nessus-Sicherheitslückenscanner und bietet agentenlose Unternehmenslösungen für die fortlaufende Überwachung auf Sicherheitslücken, Konfigurationsfehler, Datenlecks, Protokollverwaltung und Risikoerkennung an, um die Sicherheit im Netzwerk und die Compliance in Bezug auf Standards wie FDCC, FISMA, SANS CAG und PCI sicherzustellen. Die preisgekrönten Produkte von Tenable werden von zahlreichen Global 2000-Unternehmen und staatlichen Einrichtungen in aller Welt verwendet, um Risiken im Netzwerk proaktiv zu minimieren. Weitere Informationen finden Sie unter http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046, USA
+1 410 872 0555
www.tenable.com

Copyright © 2002-2011 Tenable Network Security, Inc.